International Journal of Research and Technology (IJRT)

International Open-Access, Peer-Reviewed, Refereed, Online Journal

ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529

| An ISO 9001:2015 Certified Journal |

Survey Paper of Distributed Denial of Service Attacks in Cybersecurity based on Machine Learning

[1]Geeta Singh, [2]Mr. Sudhir Goswami

M. Tech. Scholar, Department of Computer Science and Engineering, SORT, People's University, Bhopal, India[1]

Assistant Professor, Department of Computer Science and Engineering, SORT, People's University, Bhopal, India[2]

ABSTRACT

Distributed Denial of Service (DDoS) attacks continue to pose a significant threat to modern cybersecurity infrastructures by disrupting network services and degrading system availability. With the rapid growth of cloud computing, IoT devices, and high-speed networks, traditional rule-based and signature-based detection mechanisms have become insufficient to handle the scale and complexity of evolving DDoS attack patterns. This survey paper provides a comprehensive review of machine learning (ML)-based approaches for detecting and mitigating DDoS attacks. It systematically analyzes various supervised learning techniques, including Logistic Regression (LR), Decision Tree (DT), Random Forest (RF), and Extreme Gradient Boosting (XGBoost), along with their effectiveness in classifying network traffic as normal or malicious. The study examines different publicly available benchmark datasets, feature extraction methods, and preprocessing strategies used in recent research. Furthermore, it compares the performance of these models based on key evaluation metrics such as accuracy, precision, recall, and F1-score. The survey highlights that ensemble-based models, particularly Random Forest and XGBoost, consistently achieve higher detection accuracy and better generalization compared to traditional methods. In addition, the paper discusses current challenges such as data imbalance, real-time detection requirements, high computational cost, and adaptability to emerging attack vectors. Finally, it outlines future research directions, including the integration of deep learning techniques, hybrid models, and real-time deployment frameworks for enhanced DDoS detection. This survey contributes to a deeper understanding of ML-based cybersecurity solutions and provides insights for developing more robust, scalable, and efficient intrusion detection systems.

Keywords- Denial of service (DoS), Machine Learning, Attack

1. INTRODUCTION

The rapid advancement of digital technologies, including cloud computing, Internet of Things (IoT), and high-speed communication networks, has significantly increased the dependency of modern society on online services. However, this growing reliance has also expanded the attack surface for cyber threats, among which Distributed Denial of Service (DDoS) attacks remain one of the most severe and disruptive. A DDoS attack aims to overwhelm a target system, server, or

network by flooding it with massive volumes of malicious traffic generated from multiple distributed sources, rendering the service unavailable to legitimate users. These attacks not only cause service downtime but also lead to substantial financial losses, reputational damage, and reduced user trust, especially for organizations that rely heavily on continuous online availability [1, 2].

Traditional DDoS detection and mitigation techniques, such as firewalls and signature-based intrusion detection systems, are often inadequate in dealing with modern attack scenarios. These conventional approaches rely on predefined rules and known attack patterns, making them less effective against sophisticated, dynamic, and previously unseen attack strategies. Additionally, the increasing scale and diversity of network traffic further complicate the identification of malicious behavior, as attack traffic can closely resemble legitimate user activity [3].

In recent years, machine learning (ML) has emerged as a promising solution for enhancing cybersecurity mechanisms due to its ability to automatically learn patterns from large datasets and adapt to new threats. ML-based approaches enable intelligent classification of network traffic by analyzing various features such as packet size, flow duration, and protocol behavior. Supervised learning techniques, including Logistic Regression (LR), Decision Tree (DT), Random Forest (RF), and Extreme Gradient Boosting (XGBoost), have been widely explored for DDoS detection due to their effectiveness in classification tasks. While Logistic Regression provides a simple and interpretable baseline, Decision Tree offers rule-based decision-making, and ensemble methods like Random Forest and XGBoost significantly improve detection accuracy by combining multiple models and reducing overfitting [4, 5].

This survey paper aims to provide a comprehensive review of machine learning-based techniques for detecting DDoS attacks in cybersecurity. It examines various datasets, preprocessing methods, feature selection techniques, and classification models used in recent studies. Furthermore, the paper compares the performance of different algorithms based on evaluation metrics such as accuracy, precision, recall, and F1-score, highlighting their strengths and limitations. The survey also addresses key challenges, including data imbalance, scalability, computational complexity, and real-time implementation requirements. By analyzing current research trends and identifying research gaps, this study seeks to guide future developments in designing more robust, efficient, and adaptive DDoS detection systems capable of addressing the evolving landscape of cyber threats [6].

2. LITERATURE REVIEW

A. A. Alashhab et al. [1], proposed an advanced framework for enhancing DDoS attack detection and mitigation in Software-Defined Networking (SDN) environments using an ensemble online machine learning model. Their work emphasizes the dynamic nature of SDN, where centralized control provides flexibility but also introduces vulnerabilities to large-scale attacks. The authors

integrated multiple online learning algorithms to build an adaptive ensemble model capable of learning from streaming network data in real time. This approach allows the system to continuously update itself as new attack patterns emerge, thereby improving detection accuracy and reducing response time. Experimental results demonstrated that the proposed ensemble model significantly outperforms traditional single-model approaches in terms of accuracy, precision, and recall, while also maintaining low computational overhead. Additionally, the study highlights the importance of combining detection with mitigation strategies, ensuring that once an attack is identified, immediate countermeasures can be applied to maintain network stability and performance.

A. Hussain et al. [2], introduced a hybrid intrusion detection system (IDS) that combines rule-based techniques with machine learning methods for detecting DDoS attacks in Cyber-Physical Production Systems (CPPS). Their approach leverages the strengths of rule-based systems in identifying known attack signatures and machine learning models in detecting unknown or evolving threats. The integration of these two paradigms results in a more robust and flexible detection mechanism capable of handling both static and dynamic attack patterns. The authors validated their model using real-world industrial datasets and demonstrated improved detection rates with reduced false positives compared to standalone approaches. The study also highlights the critical need for secure and reliable IDS solutions in industrial environments, where disruptions can lead to severe operational and financial consequences.

C. S. Shieh et al. [3], addressed the challenge of detecting unknown or zero-day DDoS attacks by proposing an open-set recognition framework based on reciprocal points learning. Unlike traditional classification methods that assume all classes are known during training, their model is designed to identify previously unseen attack types by distinguishing them from known classes. This approach significantly enhances the adaptability and robustness of DDoS detection systems, especially in rapidly evolving threat landscapes. The authors demonstrated that their method achieves superior performance in identifying unknown attacks while maintaining high accuracy for known classes. This work contributes to the development of more intelligent and resilient cybersecurity systems capable of handling uncertainty and novelty in attack patterns.

S. Naiem et al. [4], focused on improving the efficiency of the Gaussian Naïve Bayes classifier for DDoS detection in cloud computing environments. Their research introduced enhancements in feature selection and data preprocessing to address issues such as data imbalance and noise, which often degrade classifier performance. By optimizing these aspects, the authors were able to significantly improve the accuracy and reliability of the Naïve Bayes model. The study demonstrated that even relatively simple machine learning algorithms can achieve competitive performance when properly optimized, making them suitable for resource-constrained environments where computational efficiency is critical.

G. W. de Oliveira et al. [5], explored an intelligent approach to mitigating DDoS attacks in Industrial Internet of Things (IIoT) environments through optimized Virtual Network Function (VNF) placement. Instead of focusing solely on detection, their work integrates network management strategies with machine learning to proactively reduce the impact of attacks. By strategically placing VNFs within the network, the system can efficiently filter malicious traffic and maintain service availability. The proposed method uses optimization techniques to balance resource utilization and security requirements, demonstrating improved resilience against DDoS attacks in complex industrial networks.

K. Muthamil Sudar et al. [6], investigated the detection of DDoS attacks in SDN using machine learning techniques, highlighting the advantages of centralized network control in enabling efficient traffic monitoring and analysis. Their study evaluated multiple ML algorithms and demonstrated that machine learning-based detection systems can effectively identify abnormal traffic patterns associated with DDoS attacks. The results showed improved detection accuracy and faster response times compared to traditional methods, emphasizing the potential of ML in enhancing SDN security.

Muthamil Sudar et al. [7], proposed a two-level security mechanism for detecting DDoS flooding attacks in SDN environments using entropy-based analysis and the C4.5 decision tree algorithm. The first level uses entropy measures to detect anomalies in traffic distribution, while the second level applies classification techniques to confirm the presence of an attack. This layered approach improves detection accuracy and reduces false positives by combining statistical analysis with machine learning. The study demonstrates the effectiveness of hybrid techniques in addressing the limitations of single-method approaches.

Dong et al. [8], presented an improved K-Nearest Neighbor (KNN) based method for detecting DDoS attacks in SDN, incorporating a mechanism to measure the degree of attack intensity. Their approach enhances the traditional KNN algorithm by introducing additional parameters that help differentiate between normal and malicious traffic more effectively. The proposed method achieved higher detection accuracy and better classification performance, particularly in identifying varying levels of attack severity.

Dong et al. [9], provided a comprehensive survey of DDoS attacks in SDN and cloud computing environments, analyzing various attack types, detection techniques, and mitigation strategies. The study highlights the vulnerabilities of modern network architectures and the challenges associated with securing them against large-scale attacks. It also emphasizes the growing role of machine learning and artificial intelligence in developing adaptive and scalable defense mechanisms.

Gu et al. [10], proposed a semi-supervised K-means clustering approach for DDoS detection using a hybrid feature selection algorithm. Their method combines supervised and unsupervised learning techniques to improve classification performance, particularly in scenarios with limited labeled data. The hybrid feature selection process enhances the quality of input data, leading to better clustering and more accurate detection of malicious traffic. The results demonstrate the effectiveness of semi-supervised learning in addressing data scarcity issues in cybersecurity applications.

3. DENIAL OF SERVICE

Denials of service attacks are significant in networks than other areas that target the availability goal of security. The threats introduced by such attacks on continued service may be either accidental or malicious.

Attack types:- There are different types of Denial-of-Service attacks that occur in different forms such as transmission failures, flooding of numerous connection, echo-chargen, ping of death, smurf, syn flood, tear drop, redirection of traffic, DNS attacks etc. Transmissions fail for many reasons. One common reason could be, the line is cut or a noise can make a packet unrecognizable or deliverable. A communicating machine along the transmission path could fail due to hardware or software reasons or have gone for repair or testing. A machine could be overloaded or saturated and due to that it cannot accept packets, until it clears its packets. These problems could be temporary or automatically fixed. Some communication failures such as break in single communication line to a computer cannot be easily repaired, and can be fixed only by forming an alternative link or repairing the damaged one. This can be viewed from malicious stand point that anyone can sever, interrupt of overload capacity to deny service [9, 10].

Failures also could occur due to the nonfunctioning of routers, circuit boards, firewalls, monitoring devices, storage devices and switches, for which age, factory flaws, power surges, heat and tampering can be the reasons. Such component failures may cause the entire network to fail. Even-though such failures are almost natural occurrences, one should also think about the possibilities of them being induced. Flooding is the most common type of attack reported to CERT/CC. It involves sending of an excessive amount of packets to the destination causing an excessive amount of end point, too much of bandwidth consumption, and hogging of a link. Both single source against single destination and multiple sources against multiple destinations are common [11].

There are different packet types that are used for attacks by attack tools. There are different types of flooding attacks that are carried out practically. The most common ones are TCP flooding, where a stream of TCP packets with various flags set are sent to the victim IP address. Syn, ACK and RST are the most common types of flags that are used for this kind of attack. UDP flooding

International Journal of Research and Technology (IJRT)

International Open-Access, Peer-Reviewed, Refereed, Online Journal

ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529

| An ISO 9001:2015 Certified Journal |

is another kind of flooding attack where stream of UDP packets are sent to the victim IP address [12].

4. DISTRIBUTED DENIAL OF SERVICE (DDOS)

DDoS attacks are two stage attacks constructed by the attackers for multiplying the effect. The first stage concentrates on planting an unnoticeable Trojan horse that may be named for a popular editor or utility on a target machine. The same may be subsequently repeated on many targets, thus making the targets systems as zombies [13]. Then a signal is sent to all zombies to launch the attack, and the victim is led to defend 'n'attacks from 'n' number of zombies, each targeting with different kind of attacks such as syn, smurf , all acting at once. DDoS attacks are considered serious due to their nature of being launched through scripts, where one can easily write procedures for planting Trojan horse to launch one or all the attacks [14]. At the outset, these attacks can be divided into two broad categories as agent handler model and Internet Relay Chat model (IRC). The agent handler model gets further divided into client-handler communication and agent-handler communication, and the IRC model gets divided to secret/private channel and public channel.

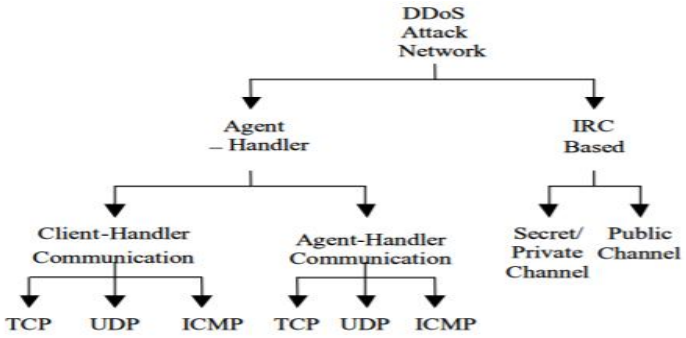

Fig. 1: DDoS Attack Network

5. MACHINE LEARNIN

Machine Learning is a subset of Artificial Intelligence concerned with "teaching" computers how to act without being explicitly programmed for every possible scenario. The central concept in Machine Learning is developing algorithms that can self-learn by training on a massive number of inputs. Machine learning algorithms are used in various applications, such as email filtering and computer vision, where it is difficult or infeasible to develop conventional algorithms to perform the needed tasks [13]. Machine learning enables the analysis of vast amounts of information. While it usually delivers faster, more precise results to identify profitable prospects or dangerous risks, it may also require additional time and assets to train it appropriately. Merging machine learning with AI and perceptive technologies can make it even more effective in processing vast volumes of information. Machine learning is closely associated with computational statistics, which focuses on making predictions using computers. Machine learning

approaches are conventionally divided into three broad categories, namely Supervised Learning, Unsupervised Learning & Semi-supervised Learning, depending on the nature of the "signal" or "feedback" available to the learning system [14].

Supervised Learning

A model is trained through a process of learning in which predictions must be made and corrected if those predictions are wrong. The training process continues until a desired degree of accuracy is reached on the training data. Input data is called training data and has a known spam / not-spam label or result at one time.

Unsupervised Learning

By deducting the structures present in the input data, a model is prepared. This may be for general rules to be extracted. It may be through a mathematical process that redundancy can be systematically reduced, or similar data can be organized. There is no labeling of input data, and there is no known result.

Semi-Supervised Learning

Semi-supervised learning fell between unsupervised learning (without any labeled training data) and supervised learning (with completely labeled training data). There is a desired problem of prediction, but the model needs to learn the structures and make predictions to organize the data. Input data is a combination of instances that are marked and unlabeled.

6. CONCLUSION

In conclusion, the survey of Distributed Denial of Service (DDoS) attack detection techniques based on machine learning highlights the significant progress made in developing intelligent and adaptive cybersecurity solutions. The reviewed studies demonstrate that traditional detection methods are increasingly inadequate in handling the scale, complexity, and evolving nature of modern DDoS attacks. Machine learning approaches, including Logistic Regression, Decision Tree, Random Forest, XGBoost, KNN, and Naïve Bayes, have shown strong potential in accurately identifying malicious traffic by learning complex patterns from network data. Among these, ensemble methods and hybrid models consistently outperform individual algorithms in terms of accuracy, precision, recall, and robustness.

Furthermore, the integration of advanced concepts such as online learning, open-set recognition, semi-supervised learning, and hybrid rule-based systems has significantly enhanced the capability of intrusion detection systems to detect both known and unknown attack patterns. The application of machine learning in emerging environments such as Software-Defined Networking (SDN), cloud computing, and Industrial IoT (IIoT) further demonstrates its versatility and effectiveness in real-world scenarios. However, several challenges remain, including data imbalance, high computational requirements, lack of real-time implementation, and the need for scalable and adaptive models.

Overall, this survey emphasizes that machine learning-based approaches are essential for building next-generation DDoS detection systems. Future research should focus on integrating deep learning techniques, improving real-time detection capabilities, and developing lightweight yet highly accurate models suitable for deployment in dynamic network environments. By addressing these challenges, more robust, efficient, and scalable cybersecurity solutions can be developed to effectively mitigate the growing threat of DDoS attacks.

REFERENCES

[1] A. A. Alashhab, M. S. Zahid, B. Isyaku, A. A. Elnour, W. Nagmeldin, and A. Abdelmaboud, "Enhancing DDoS Attack Detection and Mitigation in SDN Using an Ensemble Online Machine Learning Model," IEEE Access, vol. 12, pp. 51630–51649, Apr. 2024.

[2] A. Hussain, E. M. Tordera, X. Masip-Bruin, and H. C. Leligou, "Rule-Based With Machine Learning IDS for DDoS Attack Detection in Cyber-Physical Production Systems (CPPS)," IEEE Access, vol. 12, pp. 114894–114911, Aug. 2024.

[3] C. S. Shieh, F.-A. Ho, M.-F. Horng, T.-T. Nguyen, and P. Chakrabarti, "Open-Set Recognition in Unknown DDoS Attack Detection With Reciprocal Points Learning," IEEE Access, vol. 12, pp. 56461–56476, Apr. 2024.

[4] S. Naiem, A. E. Khedr, A. M. Idrees, and M. I. Marie, "Enhancing the Efficiency of Gaussian Naïve Bayes Machine Learning Classifier in the Detection of DDoS in Cloud Computing," IEEE Access, vol. 11, pp. 124597–124608, Oct. 2023.

[5] G. W. de Oliveira, M. Nogueira, A. L. dos Santos, and D. M. Batista, "Intelligent VNF Placement to Mitigate DDoS Attacks on Industrial IoT," IEEE Trans. Network and Service Management, vol. 20, no. 2, pp. 1319–1331, Jun. 2023.

[6] K. Muthamil Sudar, M. Beulah and P. Deepalakshmi, "Detection of Distributed Denial of Service Attacks in SDN using Machine learning techniques", International Conference on Computer Communication and Informatics (ICCCI), Jan. 27 – 29, 2021, Coimbatore, INDIA.

[7] Muthamil Sudar, K., & Deepalakshmi, P. (2020). A two level security mechanism to detect a DDoS flooding attack in software-defined networks using entropy-based and C4. 5 technique. Journal of High Speed Networks, (Preprint), 1- 22.

[8] Dong, S., & Sarem, M. (2019). DDoS Attack Detection Method Based on Improved KNN With the Degree of DDoS Attack in Software-Defined Networks. IEEE Access, 8, 5039-5048.

[9] Dong, S., Abbas, K., & Jain, R. (2019). A survey on distributed denial of service (DDoS) attacks in SDN and cloud computing environments. IEEE Access, 7, 80813- 80828.

[10] Gu, Y., Li, K., Guo, Z., & Wang, Y. (2019). Semisupervised K-means DDoS detection method using hybrid feature selection algorithm. IEEE Access, 7, 64351- 64365.

[11] A. Raghavan, F. D. Troia, and M. Stamp, ``Hidden Markov models with random restarts versus boosting for malware detection," J. Comput. Virol. Hacking Techn., vol. 15, no. 2, pp. 97107, Jun. 2019.

[12] T. Young, D. Hazarika, S. Poria, and E. Cambria, ``Recent trends in deep learning based natural language processing [review article]," IEEE Comput. Intell. Mag., vol. 13, no. 3, pp. 5575, Aug. 2018.

[13] X. Lei and Y. Xie, ``Improved XGBoost model based on genetic algorithm for hypertension recipe recognition," Comput. Sci, vol. 45, pp. 476481, 2018.

[14] Y. Guo, Y. Liu, A. Oerlemans, S. Lao, S. Wu, and M. S. Lew, ``Deep learning for visual understanding: A review," Neurocomputing, vol. 187, pp. 2748, Apr. 2016.

[15] Abduvaliyev, A., Pathan, A.-S. K., Zhou, J., Roman, R., and Wong, W.-C. “On the Vital areas of Intrusion Detection Systems in Wireless Sensor Networks”, IEEE Communications Surveys & Tutorials, Vol. 15, Issue 3, pp. no. 1223–1237, 2015.