A Fuzzy approach for DDoS attack detection in Digital Forensics

RESHMA A S

Assistant Professor,SRM IST Ramapuram.

1. Introduction

Denial of Service (DoS) attacks are presumed to be severe threats on the web, which aim to hinder the network's bandwidth, thus disrupting the network operations (Cheema et al., 2022). The DoS attacks involve the operation interruption of a system/network/service. It happens through a single-source attack (Syed et al., 2020). Distributed denial of service attack (DDoS), a sub-category of DoS, is confronted by multiple sources to compromise the network (Agrawal & Vieira, 2013; Mittal et al., 2023). In DDoS attacks, cybercriminals often target firewalls, routers, and links, causing damage to the victim's defense system either for ransom or personal target (Bawany et al., 2017). This attack often results in enormous losses for the sector involved in online services. In this context, digital forensics, a category of online service, is a practical approach for cyber specialists in gathering digital evidence to uncover fraudulent activities in online media; it is also prone to cyber-attacks. Malicious intruders in this situation often target digital forensic experts' tools; however, a DoS attack is widespread and tampers with the forensic investigation process. This issue highlights the need for an immediate approach to confront the DoS/DDoS issue posed by cybercriminals (Pandey et al., 2020). DDoS attacks have been in research studies for many decades; nevertheless, intense aftereffects were understood after witnessing the disruption of popular websites Amazon, Spotify, and Twitter in 2016 by DDoS attacks (*Twitter, Amazon, Spotify Went down Following Massive DDoS Attack*, 2016). This paper proposes to employ fuzzy logic, which can act as a countermeasure with its power to identify malicious packets and, therefore, take proper actions in preventing DDoS attacks (Iyengar et al., 2014). A DoS/DDoS attack is considered the most dangerous among other cyber threats, for which disruption technology like machine learning has been employed in identifying DDoS attacks to guarantee multilayer privacy concerns (Kumari & Mrunalini, 2022).

1.1 Research Problem

Data monitoring is the most critical factor in digital forensics and also an aspect to be safeguarded from cyberattacks, mainly distributed denial of service (DDoS). DDoS detection has been under research for several decades (Tushir et al., 2021). The existing literature studies presented approaches to avoid DDoS attacks that lack broader applicability detection and recovery, focusing only on metrics like packet size and energy consumption and overlooking critical factors like inter-node communication patterns and network congestion (Pajila et al., 2021; Rios et al., 2021). Also, the traditional approaches to prevent DDoS attacks from accessing large data sets are appropriate. For this reason, researchers started adopting machine learning algorithms to detect DDoS attacks (Al-Shareeda et al., 2023; Awan et al., 2021). Despite the advancement of study in this sector, broader application in DDoS detection models is required. The limitation of the current studies is that they may fail to detect and respond to DDoS attacks, which further evade the detection mechanism.

1.2 Research Questions

1. How can inter-node communication patterns and network congestion metrics help to enhance the accuracy of a DDoS attack detection system?
2. How can implementing machine learning algorithms in fuzzy logic systems improve DDoS attack detection?
3. What specific data sets are effective for training machine learning models in identifying DDoS attacks?

1.3 Aims and Objectives

This study aims to develop a fuzzy logic DDoS detection integrating machine learning algorithms to improve the reliability and accuracy of DDoS detection. This study addresses the research gap by incorporating inter-node communication and network congestion metrics.

1. To develop intrusion detection for DDoS attacks suitable for the digital forensics sector.
2. To develop fuzzy logic rule sets to identify DDoS attacks in digital forensics to classify malicious networks accurately considering the metric inter-node communication patterns and network congestion.
3. To design and implement fuzzy logic combined with machine learning algorithms to improve the DDoS attack detection accuracy.
4. To train machine learning models on normal and malicious traffic to enhance the DDoS detection accuracy.
5. To develop a real-time monitoring system using ML algorithms to identify network traffic.

2. Research Methodology

2.1 Literature Review

This section comprehensively reviews existing studies on DDoS and the approaches to detect them. This section assists in identifying the research gaps and addressing them by developing a novel framework for this research work.

2.2 DDoS Detection System Fuzzy Logic Combined with Machine Learning

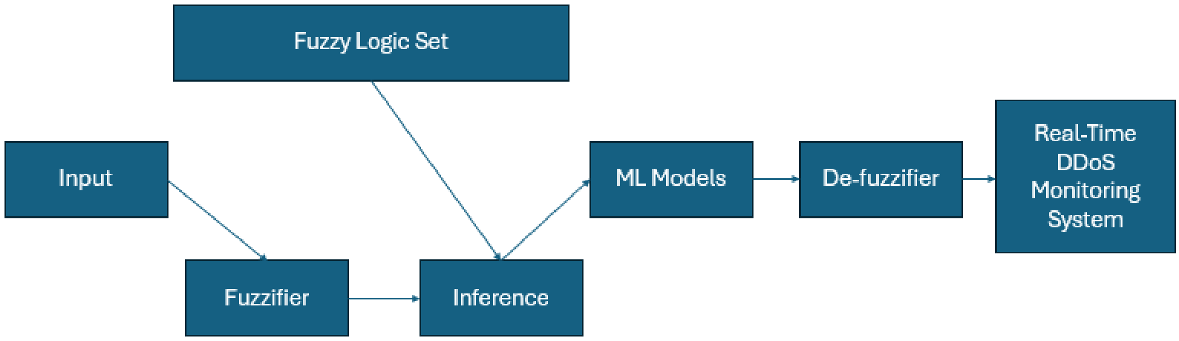

Figure 2.1: DDoS detection system integrating fuzzy logic with machine learning

2.2.1 Data Collection

To develop a fuzzy logic rule set for DDoS detection, the data is taken from sources that include both malicious and legitimate network traffic. This study uses network traffic data from Kaggle to train the model.

2.2.2 Data Preprocessing

The data is cleaned and preprocessed to remove noise and add the missing values. The data is normalized to ensure consistency in datasets.

2.2.3 Feature Extraction

This study extracts relevant features from the preprocessed data, exclusively packet size, packet rate, network congestion, and inter-code communication patterns. A fuzzy logic rule set will be developed to classify legitimate and malicious traffic based on the features.

2.2.4 Fuzzy Logic Rule Set Development

Identify the various factors that trigger a DDoS attack. Classify the data with various descriptive labels into fuzzy sets. With a membership function for each fuzzy set, apply fuzzy rules with an "If-then" loop. Further, input values are converted into fuzzy values through the membership functions (Pajila et al., 2021).

2.2.5 Machine Learning Integration

The values obtained from the previous step are used to create a dataset for training machine learning models. Choose the appropriate machine learning algorithms to identify the DDoS attacks. Train the machine learning models using the fuzzy logic rule to learn the DDoS attack pattern. This approach guarantees the multi-layered detection of DDoS attacks (Rios et al., 2021).

2.2.6 Model Evaluation

The model developed its performance and is evaluated based on recall, F-1 score, and precision. Further, fuzzy logic is combined with the machine learning model and the traditional methods (Rios et al., 2021).

2.2.7 Real-Time DDoS Monitoring System

Implement trained machine learning models and fuzzy logic rules to identify the real-time network. Translate the fuzzy outputs to the values (defuzzification) to decide whether the network traffic is legitimate/malicious.

3. Research Timeline

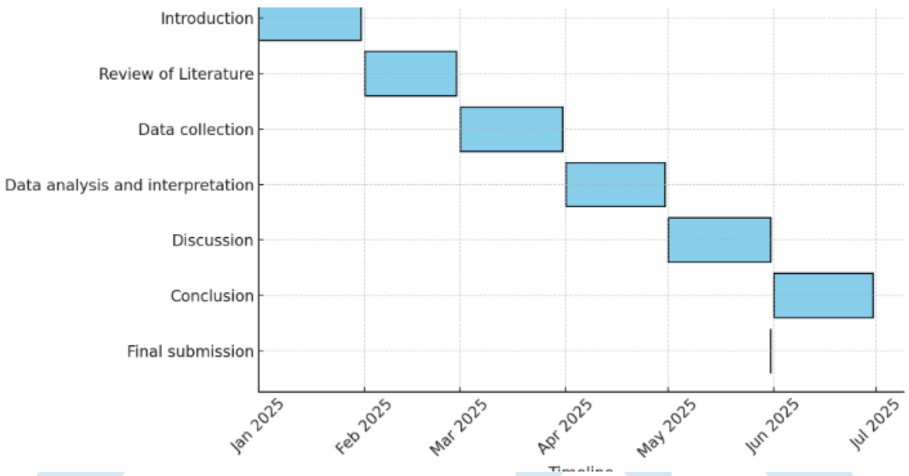

Figure 3.1: Research Timeline

The project study delivery phases are systematically represented in the Gantt chart. This Gantt chart assists in identifying the progression of the study and facilitating efficient management.

References

Agrawal, S., & Vieira, D. (2013). A survey: DDOS Attack on Internet of Things. *Abak{ó}s, Belo Horizonte*, *1*(2), 78–95.

Al-Shareeda, M. A., Manickam, S., & Saare, M. A. (2023). DDoS attacks detection using machine learning and deep learning techniques: analysis and comparison. *Bulletin of Electrical Engineering and Informatics*, *12*(2), 930–939. https://doi.org/10.11591/eei.v12i2.4466

Awan, M. J., Farooq, U., Babar, H. M. A., Yasin, A., Nobanee, H., Hussain, M., Hakeem, O., & Zain, A. M. (2021). Real-time ddos attack detection system using big data approach. *Sustainability (Switzerland)*, *13*(19), 1–19. https://doi.org/10.3390/su131910743

Bawany, N. Z., Shamsi, J. A., & Salah, K. (2017). DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions. *Arabian Journal for Science and Engineering*, *42*(2), 425–441. https://doi.org/10.1007/s13369-017-2414-5

Cheema, A., Tariq, M., Hafiz, A., Khan, M. M., Ahmad, F., & Anwar, M. (2022). Prevention Techniques against Distributed Denial of Service Attacks in Heterogeneous Networks: A Systematic Review. *Security and Communication Networks*, *2022*. https://doi.org/10.1155/2022/8379532

Iyengar, N. C. S. N., Banerjee, A., & Ganapathy, G. (2014). A fuzzy logic based defense mechanism against distributed denial of service attack in cloud computing environment. *International Journal of Communication Networks and Information Security*, *6*(3), 233–245. https://doi.org/10.17762/ijcnis.v6i3.864

Kumari, K., & Mrunalini, M. (2022). Detecting Denial of Service attacks using machine learning algorithms. *Journal of Big Data*, *9*(1). https://doi.org/10.1186/s40537-022-00616-0

Mittal, M., Kumar, K., & Behal, S. (2023). Deep learning approaches for detecting DDoS attacks: a systematic review. *Soft Computing*, *27*(18), 13039–13075. https://doi.org/10.1007/s00500-021-06608-1

Pajila, B., Julie, E. G., & Robinson, Y. H. (2021). *FBDR-Fuzzy based DDoS attack Detection and Recovery mechanism for wireless sensor networks*.

Pandey, A. K., Tripathi, A. K., Kapil, G., Singh, V., Khan, M. W., Agrawal, A., Kumar, R., & Khan, R. A. (2020). *Current Challenges of Digital Forensics in Cyber Security*. 31–46. https://doi.org/10.4018/978-1-7998-1558-7.ch003

Rios, V. de M., Inácio, P. R. M., Magoni, D., & Freire, M. M. (2021). Detection of reduction-of-quality DDoS attacks using Fuzzy Logic and machine learning algorithms. *Computer Networks*, *186*. https://doi.org/10.1016/j.comnet.2020.107792

Syed, N. F., Baig, Z., Ibrahim, A., & Valli, C. (2020). Denial of service attack detection through machine learning for the IoT. *Journal of Information and Telecommunication*, *4*(4), 482–503. https://doi.org/10.1080/24751839.2020.1767484

Tushir, B., Dalal, Y., Dezfouli, B., & Liu, Y. (2021). A Quantitative Study of DDoS and E-DDoS Attacks on WiFi Smart Home Devices. *IEEE Internet of Things Journal*, *8*(8), 6282–6292. https://doi.org/10.1109/JIOT.2020.3026023

Twitter, Amazon, Spotify went down following massive DDoS attack. (2016). Indian Express. https://indianexpress.com/article/technology/tech-news-technology/major-websites-like-twitter-amazon-went-down-after-massive-ddos-attack-3096207/