Recognizing Network Threats Using Machine Learning: A Comprehensive Overview

DEEN MOHD[1], MOHD VAKIL[2]
[1, 2]*Department of Computer Science and Engineering, R D Engineering College, Ghaziabad, India*

Abstract- ***The number of intelligent devices has increased at an unprecedented rate over the last ten years, and the spread of intelligent machines has increased dramatically in recent years. In order to guarantee constant communication amongst networked IoT devices, computer networks are essential. Unfortunately, the significant rise in the usage of smart devices has opened the door for significant unethical behavior within networks. The primary network danger under investigation in this study is the "Low Rate/Slow Denial of Service (LDoS) attack," which seriously jeopardizes the integrity of the internet. Due to the fact that these assaults do not produce large amounts of bandwidth or abrupt increases in network activity, identifying their source is quite difficult. This study investigates the use of machine learning to improve the detection.***

Indexed Terms— LDoS attack, DDoS attack, Anomaly detection, ML, RL, IDS, Hyper parameter optimization

I. INTRODUCTION

In today's digital age, the rapid growth of technology demands robust security and privacy measures. The Internet of Things (IoT), while revolutionizing connectivity, introduces significant vulnerabilities. Many IoT devices lack fundamental security features, making them prime targets for cyberattacks—particularly Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks. DoS attacks aim to disrupt a device or network's availability by overwhelming it with traffic, thereby denying legitimate users access. When executed through botnets like Mirai using multiple compromised devices, these attacks become DDoS, posing a serious threat to critical internet infrastructure. For instance, a smart home with ten connected devices could unknowingly participate in a DDoS attack. This highlights the danger of unsecured IoT ecosystems. This study focuses on Low-Rate Denial-of-Service (LDoS) attacks—stealthy, targeted disruptions that degrade network performance while evading traditional detection mechanisms.

1.1 Importance of the study

Despite the implementation of numerous security strategies, modern networks remain vulnerable—particularly to stealthy threats like Low-Rate Denial-of-Service (LDoS) attacks. Traditional defenses often struggle to detect and mitigate these subtle intrusions, as they are designed to exploit system vulnerabilities gradually and covertly. Therefore, there is a growing need for security frameworks that can handle unpredictable network behavior and adapt to evolving attack vectors. LDoS attacks differ from traditional DDoS attacks by using low, continuous traffic patterns to gradually exhaust system resources. These attacks often target protocol-level weaknesses, making detection difficult and allowing the attacker to degrade system performance over time. Figure 1 illustrates a typical LDoS scenario.

Machine learning, a subfield of artificial intelligence, enables systems to learn from data and make autonomous decisions without explicit programming. It has become a critical tool in cybersecurity, as shown in Figure 2, with applications ranging from intrusion detection to anomaly detection in complex network environments.

.

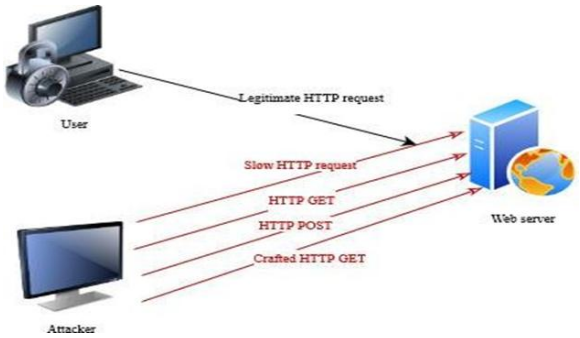

Figure 1. Low-rate DoS attack Scenario

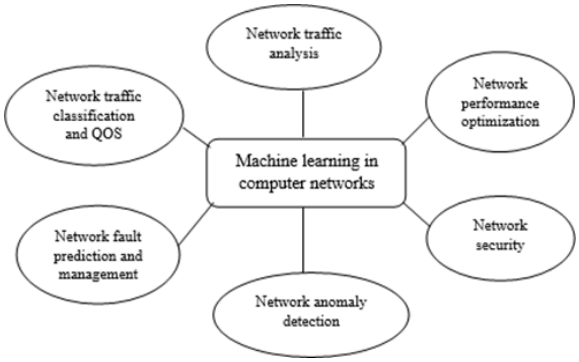

Fig. 2 Applications of machine learning within the realm of cyber security

Machine learning (ML) techniques play a vital role in identifying malicious traffic within Intrusion Detection Systems (IDS). These systems rely on ML classifiers—algorithms trained to recognize patterns in data—to categorize traffic and detect anomalies. In the context of IDS, classifiers are trained using datasets containing various attack types, enabling them to identify unusual behavior in real-time traffic. While traditional Denial-of-Service (DoS) attacks generate noticeable spikes in network activity, Low-Rate DoS (LDoS) attacks are more subtle. These attacks operate through intermittent bursts of low-rate traffic, making them harder to detect. Typically, LDoS bursts represent just 10–20% of normal traffic levels, effectively blending in with legitimate data streams. This stealthy approach not only complicates detection but also significantly degrades the victim's throughput over time. Given their prolonged and inconspicuous nature, LDoS attacks pose a serious challenge to current security measures. Thus, there is an urgent need to develop new, intelligent detection methods capable of identifying such attacks within dynamic and complex network environments.

II. MACHINE LEARNING IN CYBER SECURITY

Table 1 shows different types of 'LDoS' attacks and attack target. Method of exploiting an attack is specified for each type of attack.

Table 1. Types of LDoS attacks

S.No	Attack type	Target	Method
1	Slow read attack	Servers	Sending requests that are intentionally slow to read
2	RUDY	HTTP/H TTPs protocols	Send HTTP requests with very slow payload, keeping connections open for extended periods and consuming server resources over time.
3	Slowloris	HTTP server	Send data slowly and consume server resources.
4	HULK	Web applications	Send many HTTP GET/POST requests and keep the server busy.
5	Apache killer	Apache web servers	Crafted HTTP GET request with long-range headers and a server consumes more memory.
6	Hash collision attack	SSL/TLS or DNS	Exploits hash collision vulnerabilities in various protocols and sends crafted inputs that generate many hash collisions.
7	Application layer protocol attacks	TCP,UDP or DNS	Exploits vulnerabilities in the protocols.

III. METHODOLOGY: ML BASED DETECTION APPROACHES

Among various defense strategies, machine learning-based methods have shown strong potential in detecting Low-Rate Denial-of-Service (LDoS) attacks due to their adaptability in cybersecurity. These AI-driven techniques are typically classified into two categories: signature-based and anomaly-based detection. The signature-based method matches incoming traffic with known attack signatures, while anomaly-based detection compares current traffic patterns against a model of normal behavior, flagging deviations as potential threats.

LDoS detection techniques are further divided into two key approaches: feature-based detection, which analyzes specific traffic characteristics, and time-frequency domain analysis, which studies traffic patterns across time and frequency to uncover hidden periodicities typical of LDoS attacks.

Despite their effectiveness, current detection methods face several challenges:

- A trade-off between detection accuracy and detection rate
- High resource consumption
- Elevated false positive and false negative rates
- Lack of adaptability to evolving threats
- Inefficiency in handling diverse and dynamic LDoS variants
- High time complexity
- Gaps between available datasets and emerging vulnerabilities
- Risks of model overfitting or underfitting

These limitations highlight the need for more robust, adaptive, and lightweight detection frameworks capable of addressing modern network threats.

IV. RESULTS AND DISCUSSION

Machine learning classifiers are frequently utilized in anomaly detection research, with dataset selection playing a critical role in model performance. In this study, the NSL-KDD dataset is employed due to its structured nature and relevance to network intrusion scenarios. This dataset includes 42 features, which are analyzed across three different types of DDoS attacks: TCP SYN, ICMP, and UDP floods. For each attack type, specific features were selected for training and evaluation.

- TCP SYN Attack: Key features include service, src_bytes, wrong_fragment, count, num_compromised, srv_count, srv_serror_rate, and serror_rate.
- ICMP Attack: Features extracted are duration, src_bytes, wrong_fragment, count, urgent, num_compromised, and srv_count.
- UDP Attack: Selected features are service, src_bytes, dst_bytes, wrong_fragment, count, num_compromised, srv_count, dst_host_srv_count, and dst_host_diff_srv_rate.

Key Observations from the Evaluation (based on Figure 3):

1. Detection accuracy for TCP and ICMP attacks is near perfect, while UDP flood attacks show noticeably lower accuracy.
2. False Positive Rate (FPR) remains a major concern in network anomaly detection systems, reflecting a trade-off between sensitivity and specificity.
3. FPR is significantly higher for UDP-based attacks, suggesting these attack patterns are more easily confused with normal traffic due to overlapping feature behavior.

These insights highlight the importance of feature selection and attack-type differentiation in improving DDoS detection models. Future work could aim to reduce FPR, particularly for protocols like UDP, by enhancing feature engineering or leveraging ensemble learning techniques.

Table 3 illustrates the confusion matrix representation for the UDP flood attack. The false positive rate is high for LR, MLP, and DT. Three out of four classifiers produce high FPR.

Table 3. Confusion matrix for UDP attack

Confusion Matrix for LR: [[2852 2005] [319 2835]]	Confusion Matrix for KNN: [[4046 811] [1237 1917]]
Confusion Matrix for MLP: [[2674 2183] [51 3103	Confusion Matrix for DT: [[3834 1023] [801 2353]]

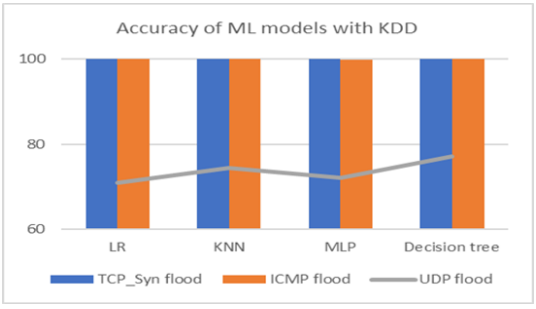

Fig. 3 Accuracy of models for different attack flows

4.1 Detection of 'DDoS attacks' using NSL-KDD dataset (Reinforcement Learning)

The NSL-KDD dataset comprises 42 features, which are utilized as the environment for training the reinforcement learning (RL) model. In this setup, each episode represents a complete interaction cycle from the initial state to a terminal state, capturing the agent's actions and resulting feedback. Rewards are granted based on the agent's predictions, while loss reflects the error between predicted and actual outcomes.

Figure 4 illustrates the model's performance over multiple episodes, highlighting trends in reward accumulation and loss reduction. As the number of episodes increases, the model achieves higher rewards and lower losses, indicating improved learning over time.

Observation: In early stages (e.g., episode 2 or 5), the model exhibits high loss and low reward, signifying initial instability in learning. This gradually stabilizes with more training episodes, suggesting the RL agent effectively adapts through experience.

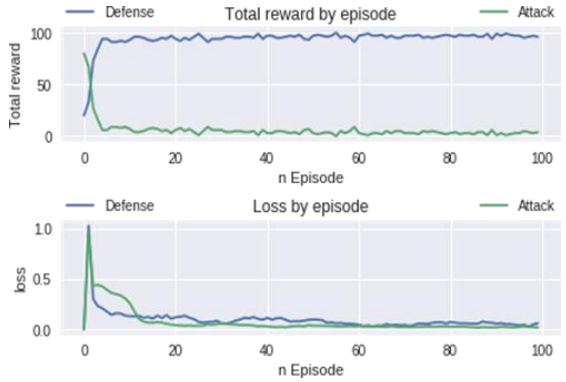

Fig. 4 Performance of RL model in terms of reward & loss

4.2 Multiclass classification of network traffic (SDN dataset)

SDN-specific (generated) datasets have been used for multi- class classification of network traffic data. There are 23 features in the dataset. All the features were considered and grouped into numerical, categorical, discrete-numerical, and continuous.

Figure 5 shows the protocol distribution statistics for malicious activity in the network. In the statistics, UDP attack flows are relatively high. When the statistics in Figure 5 and the performance in Figure 3 are compared, identification of "DDoS attacks" exploited through UDP flood is challenging.

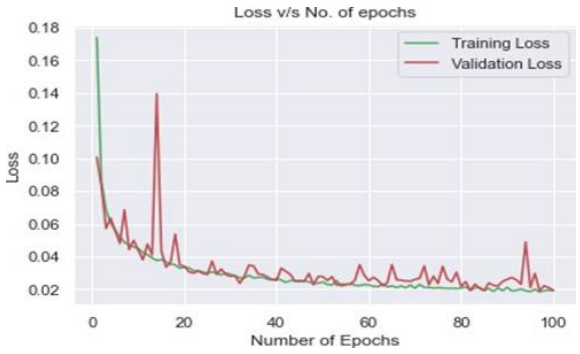

Fig. 5 Performance of ML model based on epoch count & Loss

V. CONCLUSION AND FUTURE SCOPE

5.1 Conclusion

This study explored the detection of slow Denial of Service (DoS) attacks using both traditional and machine learning-based methods. Several detection strategies—ranging from conventional techniques to deep learning and anomaly detection—were reviewed. A key challenge identified is the high false alarm rate associated with binary classification models. To overcome this, integrating reinforcement learning (RL) into hybrid systems shows strong potential for developing a more adaptive and robust Intrusion Detection and Prevention System (IDPS), capable of effectively identifying and mitigating a wider range of complex and evolving threats.

5.2 Future Scope

Detecting low-rate DoS (LDoS) attacks remains difficult due to their stealthy and gradual nature. Reinforcement Learning (RL) offers a promising solution, as it allows systems to learn and adapt based on feedback from dynamic environments. Future research should focus on:

- Applying RL to LDoS detection, where the RL agent learns optimal strategies through reward-based feedback, enabling better detection of subtle attack patterns.
- Exploring external model parameters, which, though not learned during training, significantly impact the model's generalization ability. Tuning these can improve detection accuracy.

Developing hybrid models, by:

- Investigating RL-based optimization of non-learned variables.

- Combining RL with feature-based methods such as traffic flow analysis, protocol-specific monitoring, and resource usage tracking.

Together, these future directions can enhance the system's resilience against increasingly dynamic and sophisticated network attacks.

REFERENCES

[1] Tang D, Gao C, Li X, Liang W, Xiao S and Yang Q, "A Detection and Mitigation Scheme of LDoS Attacks via SDN Based on the FSS-RSR Algorithm," IEEE Transactions on Network Science and Engineering, Vol.10, Issue.4, pp.1952 -1963, 2023, DOI: 10.1109/TNSE.2023.3236970

[2] Zhan S, Tang D, Man J, Dai R and Wang X, "Low-Rate DoS Attacks Detection Based on MAF-ADM," MDPI Sensors, Vol.20, Issue.1, pp.189, 2020, https://doi.org/10.3390/s20010189.

[3] Liang Liu, Yue Yin, Zhijun Wu, Qingbo Pan and Meng Yue, "LDoS attack detection method based on traffic classification prediction," IET information security, WILEY, Vol.16, Issue.2, pp.86-96, 2022, DOI: 10.1049/ise2.12046.

[4] Wu Zhijun, Li Wenjing, Liu Liang and Yue Meng, "Low-Rate DoS Attacks, Detection, Defense and Challenges: A Survey," IEEE access, Vol.8, pp.43920-43943, 2020, DOI: 10.1109/ACCESS.2020.2976609.

[5] Wenwen Sun, Shaopeng Guan, Peng Wang, Qingyu Wu, "A hybrid deep learning model based low-rate DoS attack detection method for software defined network," Emerging telecommunications technologies, Wiley, Vol.33, Issue.5, 2022, https://doi.org/10.1002/ett.4443.

[6] Harun Surej Ilango, Maode Ma and Rong Su, "A FeedForward– Convolutional Neural Network to Detect Low-Rate DoS in IoT," Engineering applications of artificial intelligence, Elsevier, Vol.114, 2022, https://doi.org/10.1016/j.engappai.2022.105059.

[7] Harun Surej Ilango, Maode Ma and Rong Su, "Low Rate DoS Attack Detection in IoT - SDN using Deep Learning," IEEE international conference on iThings, Australia, 2022, DOI: 10.1109/iThings - GreenCom - CPSCom - SmartData- Cybermatics53846.2021.00031

[8] Yazhi Liu, Ding Sun, Rundong Zhang and Wei Li, "A Method for Detecting LDoS Attacks in SDWSN Based on Compressed Hilbert–Huang Transform and Convolutional Neural Networks," MDPI Sensors, Vol.23, Issue.10, pp.4745, 2023, https://doi.org/10.3390/s23104745.

[9] D. Tang, S. Wang, B. Liu, W. Jin and J. Zhang, "GASF-IPP: Detection and Mitigation of LDoS Attack in SDN," IEEE Transactions on Services Computing, pp.1-12, 2023, DOI: 10.1109/TSC.2023.3266757.

[10] Xinmeng Li, Kai Zheng, Dan Tang, Zheng Qin, Zhiqing Zheng, Shihan Zhang, "LDoS Attack Detection Based on ASNNC-OFA Algorithm," IEEE wireless communications and networking conference, China, 2021, DOI: 10.1109/WCNC49053.2021.9417400

[11] Dan tang, Jingwen chen, Xiyin wang, Siqi zhang,Yudong yan, "A new detection method for LDoS attacks based on data mining," Future generation computer systems, Elsevier, Vol.16, Issue.128, pp.73-87, 2022, https://doi.org/10.1016/j.future.2021.09.039

[12] Wei shi, Dann tang, Sijia Zhan, Zheng Qin and Xiyin wang, "An approach for detecting LDoS attack based on cloud model," Forensics of computer science, Springer, Vol.16, Issue.166821, 2022, https://doi.org/10.1007/s11704-022-0486-1.

[13] Naiji Zhang; Fehmi Jaafar; Yasir Malik, "Low-Rate DoS Attack Detection Using PSD Based Entropy and Machine Learning," 6th IEEE international conference on cyber security and cloud computing, Paris, France, pp.59-62, 2019, DOI 10.1109/CSCloud/EdgeCom.2019.00020.

[14] Dan tang, Liu tang, Rui dai, Jingwen chen, Xiong Li and Joel J.P.C.Rodrigues, "MF-Adaboost: LDoS attack detection based on multi-features and improved Adaboost,", Future generation computer systems, Elsevier, Vol.106, pp.347-359, 2020, https://doi.org/10.1016/j.future.2019.12.034.

[15] Jingtang Luo, Xiaolong Yang, Jin Wang, Jie Xu,

Jian Sun and Keping Long, "On a Mathematical Model for Low-Rate Shrew," IEEE Transactions on Information Forensics and Security, Vol.9, Issue.7, pp.1069-1083, 2014.

[16] Saurabh Chauhan, Dharamveer Singh, Atul Kumar Singh (2022) "Artificial Intelligence In The Military: An Overview Of The Capabilities, Applications, And Challenges", Journal of Survey in Fisheries Sciences, Vol 9 (2) pp 984-991. https://doi.org/10.53555/sfs.v9i2.2911

[17] Kiran, Dharamveer Singh, Nitin Goyal, (2023) "Analysis Of How Digital Marketing Affect By Voice Search", Journal of Survey in Fisheries Sciences, Vol. 30 (2) 407-412. https://doi.org/10.53555/sfs.v10i3.2890

[18] Yukti Tyagi, Dharamveer Singh, Ramander Singh, Sudhir Dawra (2024) "Analysis Of The Most Recent Trojans On The Android Operating System", Educational Administration: Theory and Practice, Vol. 30(2) 1320-1327. https://doi.org/10.53555/kuey.v30i2.6846

[19] Shivanee Singh, Dharamveer Singh, Ravindra Chauhan (2023) "Manufacturing Industry: A Sustainability Perspective On Cloud And Edge Computing", Journal of Survey in Fisheries Sciences, pp 1592-1598. https://doi.org/10.53555/sfs.v10i2.2889