Journal of Information Systems Engineering and Management
2025, 10(34s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

A Brief Review of Low-Rate DDoS Attack Detection in Cloud Environments Using Soft Computing Techniques

Achsah Susan Mathew[1], Dr. Hanumanthappa M[2], Dr Nagaraju Kilari[3]
[1]*Research Scholar, Department of Computer Science, Bangalore University, Bengaluru, Karnataka, India*
[2] *Senior Professor, Department of Computer Science, Bangalore University, Bengaluru, Karnataka, India.*
[3]*Associate Professor and Hod, Department of Computer Science, New Horizon College, Marathalli, Bengaluru*

ARTICLE INFO

Received: 30 Dec 2024

Revised: 03 Feb 2025

Accepted: 12 Feb 2025

ABSTRACT

The rise of technology and the revolution of cloud computing have made scalability of services seamless but it also attracted lot of hackers aiming to misuse the sensitive data stored on the cloud. Growing cyber misconduct has turned security into a major concern for individuals, government and countries. Traditional security methods are not sufficient against new threats particularly low-rate distributed denial of service (LRDDOS) attacks can disrupt network services and disable system functionality. LRDDOS attacks are rapidly advancing posing significant detection and prevention challenges. So, this paper reviews recent advancement in LRDDOS attack detection through soft computing techniques and suggest ways to adopt these techniques for effective detection and prevention.

Keywords: Cloud Computing, Security, LRDDOS attack, Detection, Prevention, Soft Computing.

INTRODUCTION

As cyber threats have become sophisticated and complicated, research into low-rate distributed denial of service (LRDDOS) detection and security in cloud computing using soft computing techniques is becoming important. LRDDOS attacks are quite difficult to figure out and prevent because they have low traffic levels that can shake the service quality instead of overloading system with large bandwidth. These attacks frequently consist of malicious traffic bursts that mix with the normal flow of data that can cause major disruptions for both users and cloud services providers. Therefore, highlighting the necessity for efficient detection techniques [1][2]. Existing detection system has difficulty to detect LRDDOS attacks because they look like a network activity. Few datasets are available, and most of the existing datasets focus on high-rate DDoS attacks, which make it challenging to train machine learning models accurately. As these days enterprises progressively transition to cloud environment the financial and operational consequences of undetected LRDDOS attacks on the resources can be substantial, urging the development of innovative detection algorithm that incorporate soft computing techniques [2][3][4]. Soft computing methods such as Hidden Markov Models (HMM) and Random Forest classifiers have shown some promising improvements for detection capabilities by effectively identifying between malicious and legitimate traffic. Hybrid models that combine various methods have also been proposed to boost detection accuracy while reducing the false alarms. This systematic methodological evolution emphasizes the significance of using various credible datasets coupled with modern algorithms to resist the stealthy nature of LRDDOS attacks in cloud environments [5][6][7]. The importance of LRDDOS detection and security goes beyond technical issues. It has significant consequences for data integrity, system stability, and general user confidence in cloud computing environments. As cyber threats multiply continued research and innovation in detection frameworks coupled with collaboration efforts between business and academia are necessary to enhance defenses against low-rate DDOS attacks [7][8]. Fig. 1 shows the standard classification of DOS attacks based on attacks characteristics and rate of traffic flow. DDOS attacks are divided into two categories: Flood and Shrew. Among the both flood attacks can be classified as either high-rate (also known as a DDOS attack) or low-rate (also known as a flood attack, but with a transmission rate below 1000 bits per second). Their division is predicated on 1000 bits per second packet transmission rate.

A typical low-rate attack shrew's traffic makes up 10% to 20% of the network's overall traffic. Its average traffic is sufficiently low to be fully hidden in regular network traffic. Both DDOS and LDOS attacks are classified as Denial-of-service attacks both these attacking strategies and tactics are essentially different [3].

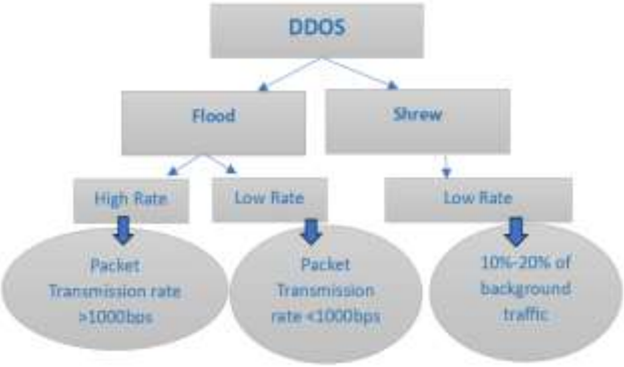
DDOS
Flood
Shrew
High Rate
Low Rate
Low Rate
Packet Transmission rate >1000bps
Packet Transmission rate <1000bps
10%-20% of background traffic

Fig.1 Classical taxonomy of DDoS

II. TYPES OF DDOS ATTACKS

Distributed Denial-of-Service (DDOS) attacks are categorized into various types based on their methods and objectives. Understanding these types is crucial for developing effective mitigation strategies.

Protocol Attacks

Protocol attacks exploit weaknesses in layer 3 (network) and layer 4 (transport) of the Open systems interconnection (OSI) model.

SYN Flood: Attackers bombard a target server with SYN requests, which causes the server to use up resources as it allots RAM for each connection that is partially open.

Ping of Death: When the target tries to reassemble the oversized packets, they are transmitted in smaller pieces overwhelming it and sometimes resulting in crashes [9].

Application Layer Attacks

Application layer assaults target OSI model layer 7 (application) they are more difficult to identify and mitigate.

HTTP Flood: Through GET or POST requests malicious actors flood a web server with HTTP requests which can cause the server to lag or stop responding.

Browser Redirection: End users are redirected to unwanted websites by this attack which degrades their experience and may compromise their data [9] [10].

Volume-based Attacks

The most prevalent type of DDOS assault is volume-based in which the attackers overload the target with traffic in an attempt to exhaust its bandwidth.

User Datagram Protocol (UDP) Flood: Attackers overload the victim's server's capacity to handle the incoming data by flooding it with UDP packets. For authorized users this may result in service interruptions.

ICMP (An Internet Control Message Protocol) Flood (Ping Flood): This attack involves sending the target a large number of ICMP echo requests which causes the server to run out of resources as it tries to reply to each request [9].

Low-rate Denial of Service (LDOS) Attacks

LDOS occurrences are harder to identify because of their smaller traffic levels. They purposefully lower the worth of service by sending brief traffic bursts that make up only 10% to 20% of the background traffic as opposed to flooding a server. This devious strategy enables the attackers to evade detection by conventional defenses [1].

Amplification Attacks

Attackers use amplification attacks to send modest requests to a third-party server that responds with a huge response by impersonating their target's IP addresses. The DNS amplification attack is the most common kind of amplification attack that uses openly accessible DNS servers to overload the target with traffic, frequently causing major service interruption [9].

Low-Rate DDOS (LRDDOS) Attacks

Low-rate Distributed Denial of Service (LDOS) attacks represent an important and growing threat to various online platforms including cloud computing services and large-scale data centers. Unlike traditional DDOS attacks which overpower the target with massive volumes of traffic to disrupt services. LDOS attacks are characterized by their ability to degrade the quality of TCP (Transmission control protocol) connections by throttling traffic to a fraction of its intended rate. These attacks typically consist of small flow bursts constituting only 10%–20% of the regular background traffic which in fact allows them to evade detection mechanisms deployed by routers and counter-DDOS solutions [1].

Detection Challenges

Due to their low traffic volume and resemblance to normal traffic patterns, LDOS attacks present special detection issues. This makes it difficult for typical detection systems to distinguish between normal shifts in network utilization and malicious activity. Existing machine learning (ML) algorithms can struggle to recognize these attacks without rich datasets that cover a extensive array of attack scenarios and attributes. Many datasets available for training detection models predominantly focus on high-rate DDOS attacks which creates a gap in the capacity to effectively train models to spot low-rate variants [2][3].

Characteristics of LDOS Attacks

The purpose of LDOS attacks is to gently interfere with services not to make it totally unusable. Attackers can efficiently hide their malicious intent by providing periodic low-rate communication that mimics normal user activity. They can damage network performance using this operational method and avoid detection by traditional detection systems. The particular methods of LDOS attacks frequently involve making use of vulnerabilities in TCP (Transmission control protocol) flows with the attack pattern consisting of controlled packet bursts meant to use up the target's bandwidth without sending out the alarms that would be associated with higher-rate attacks [1].

The Worth of Various Datasets

The variety and quality of training datasets have a significant impact on the effectiveness of detection systems. It is essential to have datasets that cover a broad range of attack types, attributes, and patterns in order to guarantee that ML models can correctly detect both high-rate and low-rate DDOS attacks. The requirement for datasets with enough features to uncover hidden patterns linked to these malicious activities is highlighted by the fact that, as several studies have shown datasets with less than ten features frequently fall short of capturing the subtle behaviors displayed during low-rate attacks [2]. Additionally, verifying the detection accuracy of these datasets before their release is vital to ensure their reliability for researchers and practitioners in the field [4].

III. SOFT COMPUTING TECHNIQUES

In cloud computing environments, soft computing techniques are essential for detecting and mitigating Low-Rate Distributed Denial of Service (DDOS) attacks. These techniques use a variety of computational models to improve security measures by correctly separating malicious traffic from legitimate data flow.

Hidden Markov Model

The Hidden Markov Model (HMM) is a crucial method used in this situation. By monitoring the data flow throughout the network, HMM makes it possible to spot trends that can point potential DDOS attacks. The dynamic character of network traffic is well captured by this probabilistic model which makes it an appropriate option for identifying irregularities linked to Low-Rate DDOS attacks [5] [7].

Random Forest Classifier

The Random Forest classifier is used to classify the detected anomalies in addition to the HMM. With the several decision trees and the aggregation of their outputs this ensemble learning technique increases the classification accuracy. By combining these two methods, a strong detection mechanism that enhances the performance of DDOS attack identification process and yielding better metrics like recall, precision, specificity, accuracy, and F-measure [5][7].

Hybrid Models and Machine Learning

To improve the accuracy of cyber intrusion detection systems recent advancements have also highlighted the use of hybrid models that blend machine learning algorithms with soft computing methods. For instance, techniques that combine genetic algorithms and Support Vector Machines (SVM) have been proposed these models effectively distinguish between legitimate data and attack traffic by utilizing clustering and flow-based characteristics [3][6].

Dataset Considerations

Access to extensive datasets for training and testing is essential to the implementation of intelligent computing methods of soft computing approaches. For researchers to properly identify hidden patterns, datasets must have a sufficient set of parameters to showcase the complexity of DDOS attacks. Furthermore, attaining adequate detection accuracy depends critically on the dataset's dependability and credibility [4]. The incorporation of well selected datasets facilitates the assessment and comparison of different suggested detection techniques leading to developments in the field.

Event Correlation-Based Approaches

Apart from model-based approaches event correlation-based techniques have become successful DDOS attack detection solutions. By examining the connections between different patterns found throughout the network these methods enable the prompt detection of malicious activity. We can improve the speed and precision of DDOS detection systems by comparing the final anomaly scores from different detection techniques [2][3].

IV. DDOS DETECTION METHODS

For detecting and reducing low-rate DDoS threats that target cloud computing environments and Software-Defined Networks (SDNs), DDOS (Distributed Denial of Service) detection techniques have grown significantly especially with the inclusion of machine learning and soft computing techniques.

Machine Learning Approaches

RDAER Model

The Robust DDOS Attack Early Response (RDAER) model is one of the prominent methods that have demonstrated high effectiveness in detecting DDOS attacks with remarkable accuracy while using only two features. This method lowers computational costs and resource utilization enabling early attack detection and effective network security through timely modifications of flow table entry rules in SDN (Software defined Controllers) [3].

Hybrid Models

There have also been proposals for hybrid models that combine supervised and unsupervised learning techniques. For instance, Najafimehr et al. [11] successfully distinguished between attack traffic and legitimate data by using clustering and other flow-based features. Another enhancement in detection approaches was introduced by Phuc

Trinh et al. [12] who combined a multivariate time series technique and Recurrent Neural Networks (RNNs) attaining a detection rate of 98.51%.

Anomaly Detection

Techniques for detecting anomalies have also become more popular. Techniques like the Deep Multi-Layer Perceptron (D-MLP) have shown remarkable results achieving detection accuracies of over 98% in a variety of attack scenarios. The D-MLP model leverages deep learning frameworks such as TensorFlow and Keras for effective classification of malicious traffic making it a formidable tool against DDOS attacks [4].

DDOS Detection in Software-Defined Networks

In a notable case study, Aladaileh et al. [13] used a Mininet emulator to establish a virtual network setup in order to assess a detection system that relying on extended Renyi joint entropy. The investigative setup consisted of an OpenFlow switch, 64 hosts, and a POX controller (Networking software written in Python). It was possible to generate both typical and unusual traffic using the Scapy hacking tool. The dataset included several UDP (User datagram protocol). DDOS attack scenarios that targeted single and multiple victim nodes resulting in seven distinct traffic profiles. It's essential to note that the dataset only included a limited amount of traffic characteristics and disregarded other DDOS attack types such as TCP and ICMP [3][4].

In a separate strategy, Tang et al. created an Intrusion Detection System (IDS) based on deep learning with the goal of identifying all kinds of intrusions with an emphasis on modern attack techniques. A collector for collecting data an anomaly detector using Deep Neural Networks (DNN), Recurrent Neural Networks (RNN) and a detection module that examines all traffic flow entries within a given time window, make this system's three primary modules. Using the NSL-KDD dataset for training and testing the system achieved a 90% detection accuracy for RNNs. But the methodology was criticized for using a dataset that did not accurately represent the features of the SDN network environment [5][7].

Deep learning techniques in anomaly-based Intrusion Detection System (IDS)

Furthermore, because deep learning approaches can dynamically learn attack patterns their progressive integration into anomaly-based intrusion detection systems has gained traction. For instance, Li et al. suggested a defensive and detection method for detecting DDoS attacks in SDN environments that makes use of Convolutional Neural Networks (CNN), RNN, and Long Short-Term Memory (LSTM) networks. Despite being restricted to high-rate DDOS attacks, their model produced verification accuracies of 98% for test data and 99% for training data [3][5].

Performance Metrics

Evaluating the performance of DDoS detection methods is critical. True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN) rates are common metrics used to assess the performance of DDoS detection methods. For instance, in high-rate attack scenarios the D-MLP approach achieved a TP rate of 98.49% while maintaining a high level of specificity at 99.94% [4].

These numbers demonstrate how well different detection techniques can reliably differentiate between malicious and genuine traffic.

Mitigation Strategies

Real-time monitoring detection systems, and documented response protocols are all necessary for the effective mitigation of DDOS attacks. Using network intrusion detection systems (IDS) like Snort () which is one of the suggested remedies. These systems can notify network administrators of ongoing attacks and assist in suspending the malicious user to reduce downtime [5][7]. Furthermore, cloud-based techniques that employ algorithms to examine traffic patterns and identify irregularities suggestive of a DDoS attack have been created [3].

Additionally, a novel framework known as RDAER (Robust DDOS Attack Early Response) has been put out emphasizing feature selection and clustering strategies to improve the detection of possible threats while maximizing computational capacity. When compared to conventional techniques this strategy can drastically lower the computing load making it scalable with the expansion of the network [2][3].

The Importance of Real-time Defense

For cloud service providers being able to identify and stop DDOS attacks instantly is essential. Given that DDOS attacks usually overwhelm their targets in a short amount of time. Automated systems that can react swiftly to such threats are crucial. This urgency is frequently difficult for current defenses to handle which highlights the need for quick and computationally effective solutions that can automatically recognize and stop attacks before they have a chance to do serious damage [2].

Comparative Analysis of Detection Models

The efficiency of the suggested RDAER model in comparison to conventional techniques is highlighted by the comparative study of detection models. The RDAER model outperformed earlier approaches, achieving a notable 99.92% higher detection accuracy and reduced detection time. Techniques including feature selection, traffic grouping, time series analysis, and event correlation are responsible for this progress therefore highlighting the importance of combining several detection tactics to improve overall performance [3][7].

V. CONCLUSION

Significant progress is anticipated in the future of low-rate Distributed Denial of Service (DDOS) detection and security in cloud computing especially with the incorporation of new technologies and approaches.

The development of advanced detection systems that make use of soft computing approaches is becoming more and more important as cloud computing continues to advance. For example, it is anticipated that the use of machine learning models, including Random Forest and Hidden Markov Models will improve the accuracy of DDOS attack detection. By enhancing their ability to categorize network traffic these models can decrease false positives and speed up response times in attack scenarios.

Enhanced Security Frameworks

One trend toward developing scalable and adaptable security solutions for cloud systems is the use of frameworks such as RDAER (Robust Detection and Adaptation for Early Response). These frameworks are made to handle networks growing size and complexity guaranteeing strong detection capabilities while preserving system speed. The optimization of these frameworks to manage multi-tiered infrastructures more effectively is probably the main focus of future study.

Integration with Network Functions Virtualization (NFV) and Software-Defined Networking (SDN)

The method to DDOS mitigation is expected to undergo a revolution with the convergence of NFV and SDN with cloud computing. In order to combat DDOS attacks these solutions provide the flexibility to dynamically assign resources and apply real-time traffic management techniques. Network administrators will be better able to identify irregularities and quickly implement countermeasures by employing software-defined architectures.

IoT (Internet of Things) and Edge Computing considerations

With the expansion of IoT devices, the security environment is becoming more challenging. Future developments will probably address the particular risks that these devices create calling for specialized DDOS detection systems that perform well in dispersed settings. Furthermore, as edge computing becomes more popular decentralized security models will be developed to address risks closer to the data sources reducing latency and improving security posture [8].

Research and Collaborative Efforts

Future trends in DDOS detection and mitigation will be greatly influenced by ongoing research. Cooperation between governmental, business, and academic institutions will make it easier to share best practices, resources, and expertise. Maintaining the resilience of cloud infrastructures against DDoS threats and staying ahead of changing attack tactics [7].

Research Article

REFRENCES

[1] https://www.techtarget.com/searchSecurity/tip/DoS-vs-DDoS-How-they-differ-and-the-damage-they-cause'. Accessed: Dec. 20, 2024.

[2] A. A. Alashhab, M. S. M. Zahid, M. A. Azim, M. Y. Daha, B. Isyaku, and S. Ali, 'A Survey of Low Rate DDoS Detection Techniques Based on Machine Learning in Software-Defined Networks', Aug. 01, 2022, MDPI. doi: 10.3390/sym14081563.

[3] W. Zhijun, L. Wenjing, L. Liang, and Y. 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.

[4] T. E. Ali, Y. W. Chong, and S. Manickam, 'Machine Learning Techniques to Detect a DDoS Attack in SDN: A Systematic Review', Applied Sciences (Switzerland), vol. 13, no. 5, Mar. 2023, doi: 10.3390/app13053183.

[5] A. V. Songa and G. R. Karri, 'An integrated SDN framework for early detection of DDoS attacks in cloud computing', Journal of Cloud Computing, vol. 13, no. 1, Dec. 2024, doi: 10.1186/s13677-024-00625-9.

[6] A. A. Bahashwan et al., 'HLD-DDoSDN: High and low-rates dataset-based DDoS attacks against SDN', PLoS One, vol. 19, no. 2 February, Feb. 2024, doi: 10.1371/journal.pone.0297548.

[7] M. S. R., 'SOFT COMPUTING BASED AUTONOMOUS LOW RATE DDOS ATTACK DETECTION AND SECURITY FOR CLOUD COMPUTING', Journal of Soft Computing Paradigm, vol. 2019, no. 2, pp. 80–90, Dec. 2019, doi: 10.36548/jscp.2019.2.003.

[8] H. Elubeyd and D. Yiltas-Kaplan, 'Hybrid Deep Learning Approach for Automatic DoS/DDoS Attacks Detection in Software-Defined Networks', Applied Sciences (Switzerland), vol. 13, no. 6, Mar. 2023, doi: 10.3390/app13063828.

[9] U. Amir and K. Hussain, 'DDoS Attacks Detection and Prevention Techniques in Cloud Computing: A Systematic Review'. [Online]. Available: https://sites.google.com/site/ijcsis/

[10] D. Tang, R. Dai, Y. Yan, K. Li, W. Liang, and Z. Qin, 'When SDN Meets Low-rate Threats: A Survey of Attacks and Countermeasures in Programmable Networks', ACM Comput Surv, Nov. 2024, doi: 10.1145/3704434.

[11] Najafimehr, Mohammad, Sajjad Zarifzadeh, and Seyedakbar Mostafavi. "A hybrid machine learning approach for detecting unprecedented DDoS attacks." The Journal of Supercomputing 78.6 (2022): 8106-8136.

[12] P. T. Dinh and M. Park, "ECSD: Enhanced Compromised Switch Detection in an SDN-Based Cloud through Multivariate Time-Series Analysis," in IEEE Access, vol. 8, pp. 119346-119360, 2020, doi: 10.1109/ACCESS.2020.3004258

[13] Bahashwan, Abdullah Ahmed, et al. "HLD-DDoSDN: High and low-rates dataset-based DDoS attacks against SDN." Plos one 19.2 (2024): e0297548.