IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

REAL TIME DETECTION AND MITIGATION OF DDOS ATTACK

Vivek Rajak, Soham Rane , Ninad Raut, Aditya Naik , Deepti Janjani

Student, Student , Student , Student, Professor

[1]Artificial Intelligence And Data Science ,

[1]Datta Meghe College of Engineering, Airoli,Navi Mumbai, India

Abstract: The context of this study is embedded in the rapid expansion of cloud computing, online service delivery, and network-dependent application growth, where Distributed Denial of Service (DDoS) attacks have emerged as a major threat to system availability and cybersecurity. In this context, DDoS attacks attempt to flood targeted systems with overwhelming traffic that eventually leads to service unavailability. Traditional defense systems often experience difficulties in providing real-time detection of DDoS attacks due to overwhelming traffic volumes and limited flexibility.

The paper proposes a real-time DDoS detection and mitigation system using packet-level traffic analysis within a windows-based firewall framework. In this context, the proposed system leverages WinDivert and Python programming languages to analyze real-time traffic in real-time. In this context, salient features of traffic are used to detect anomalies. A threshold-based detection mechanism is used to detect normal and malicious traffic.

The system also proposes immediate mitigation techniques to mitigate detected DDoS attacks. In this context, malicious packets are dropped immediately to ensure minimal impact on legitimate users. This approach is also cost-effective and does not require any specific hardware.

The experimental evaluation proves that the system is capable of achieving rapid detection speeds, lower response latency, and mitigating large-scale Distributed Denial of Service attacks. It highlights the importance of real-time packet inspections and rapid response techniques in improving network security.

The proposed technique provides a realistic and efficient technique for countering modern-day DDoS attacks and provides a foundation for further improvements by incorporating intelligent and adaptive techniques.

Keywords: DDoS Attack, Network Security, Packet Analysis, WinDivert, Real-Time Detection, Firewall, Cybersecurity

1. INTRODUCTION

In recent times, the rise of cloud computing and e-commerce sites has significantly increased the reliance on network infrastructure. However, this has concurrently increased the vulnerability of network systems to various cyber attacks, and Dis-tributed Denial of Service attacks are a major concern in this context. A Distributed Denial of Service attack is an attack that aims at exhausting a target system's resources by forcing an enormous quantity of traffic onto the system, making it im-possible for it to provide services to genuine users [1].

Distributed Denial of Service attacks have become sophisticated and can be of high-rate and low-rate varieties. In a Distributed Denial of Service attack, attackers often use bot-nets that consist of infected computers to send a huge quantity of malicious traffic from different sources. It is difficult to identify Distributed Denial of Service attacks since they are distributed and can be difficult to differentiate from genuine traffic using conventional detection systems [3].

Traditional detection systems like firewalls and intrusion detection systems mainly rely on predefined rules and signatures. Although these systems are effective in detecting conventional attacks, they are not effective in a timely manner. In addi-tion, some of these systems are expensive and cannot be implemented in small-scale environments [11].

In order to mitigate the challenges that have been identified,

a real-time detection and mitigation framework for DDoS at-tacks has been proposed in this study, which relies on packet-level traffic analysis. The framework uses WinDivert to capture packets in real-time and analyze the traffic by measuring the packet rate, source IP address behavior, and protocol distributions. In addition, a threshold-based detection technique has been used to identify anomalous traffic patterns that may be indicative of a potential attack [14].

As soon as the malicious activity has been identified, the framework uses real-time mitigation techniques to discard the suspicious packets and block the attacking IP address, thereby mitigating the attacks and facilitating the sustenance of the availability of the services. The proposed framework is lightweight, cost-effective, and practical in the real world without the need for special hardware devices.

Problem Statement: The aim of this study is to design and develop a system that can detect and prevent distributed denial-of-service attacks in real-time by analyzing the network traffic at the packet level with low latency, low false positive rate, and efficient resource usage.

Contributions:

- Design of a real-time packet-level DDoS detection system using WinDivert
- Implementation of a threshold-based anomaly detection mechanism
- Development of a lightweight and efficient mitigation strategy
- Reduction of attack impact through immediate packet filtering and IP blocking
- Improvement in network stability during high-volume at-tack scenarios

2. PROPOSED METHODOLOGY

The proposed system utilizes a real-time detection and mitigation methodology for distributed denial-of-service attacks, based on a packet-level traffic analysis. The methodology is developed to monitor network traffic, detect unusual patterns, and respond to potential attacks in real-time.

The system is composed of the following key components:

2.1 Packet Capture Layer

The system monitors the real-time incoming and outgoing net-work packets using the Windows utility ”WinDivert,” which is a packet interception utility. This provides access to low-level network traffic without the requirement of any hardware or complex configuration [10].

2.2 Traffic Feature Extraction

Each captured packet is analyzed to extract relevant features required for detection. These include:

- Source IP address and destination IP address

- Packet arrival rate per IP
- Protocol type (TCP, UDP, ICMP)
- Frequency of requests within a time window

These features are used to understand traffic behavior and identify potential anomalies.

2.3 Traffic Monitoring and Analysis

The system maintains real-time statistics of network activity, including:

- Number of packets received per second
- Requests generated by individual IP addresses
- Sudden spikes in traffic volume

A sliding time window approach is used to track traffic pat-terns over short intervals, enabling early detection of abnormal behavior.

2.4 Detection Mechanism

Threshold-based anomaly detection methodology is used in the identification of anomalous traffic. Malicious traffic is identified if the packet rate of a particular IP address or the overall network traffic crosses a predefined threshold value. Such statistical and anomaly-based detection techniques have been widely studied in network security research [14].

This methodology provides fast detection with less computational complexity, making it suitable for real-time applications.

2.5 Mitigation Strategy

Once malicious activity is detected, the system immediately performs mitigation actions:

- Dropping suspicious or excessive packets
- Blocking IP addresses generating abnormal traffic
- Preventing further communication from identified sources

This helps in reducing the impact of the attack and main-taining service availability.

2.6 Real-Time Response Mechanism

The system is designed to operate with minimal latency be-tween detection and mitigation. By processing packets in real-time, it ensures that attacks are controlled before causing sig-nificant damage to the system.

2.7 Logging and Monitoring

All detected events and actions are logged for analysis and au-diting. The logs include:

- Timestamp of attack detection
- Source IP addresses involved
- Number of blocked packets
- Mitigation actions taken

These logs can be used for further analysis and improving system performance.

2.8 System Workflow

The overall workflow of the system is as follows:

1. Capture network packets in real-time
2. Extract relevant features from each packet
3. Monitor traffic patterns and calculate statistics
4. Detect anomalies using threshold conditions
5. Apply mitigation strategies (drop/block)
6. Log events and continue monitoring

This methodology enables efficient detection and mitigation of DDoS attacks while maintaining low resource consumption and high responsiveness.

3. DDoS DETECTION AND MITIGA-TION ALGORITHM

Algorithm 1: Real-Time DDoS Detection and Mitigation

Input:

Incoming packet stream P Threshold T (packet rate limit) Time window t

Output:

Allowed traffic OR Blocked malicious t

Step 1: Initialize data structure for IP t (e.g., Hash Map: IP -> packet coun

Step 2: For each incoming packet p in P:

Step 3: Extract source IP (IP_src)

Step 4: Update packet count: count(IP_src) = count(IP_src) + 1

Step 5: Calculate packet rate: R(IP_src) = count(IP_src) / t

Step 6: If R(IP_src) > T:

Mark IP_src as malicious Add IP_src to blacklist Drop current packet

Block further packets from IP_src

Step 7: Else:

Allow packet to pass

Step 8: Reset counts periodically after time windo Step 9: Log activity:

- IP address
- Packet rate
- Action taken (Allowed/Blocked)

Step 10: Continue monitoring in real-time

Time Complexity: O(n) where n is the number of packets processed

Space Complexity: O(k) where k is the number of active IP addresses

Key Features:

- Real-time packet processing
- Sliding time window-based monitoring

- Threshold-based anomaly detection
- Dynamic IP blocking and packet filtering
- Efficient memory usage using hash-based tracking

4. SYSTEM ARCHITECTURE

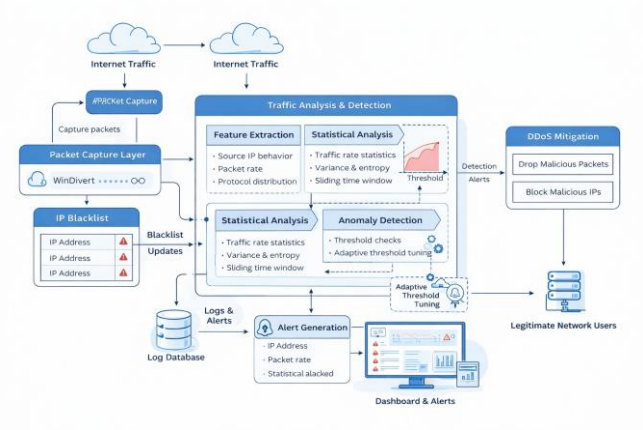

Figure 1: Proposed System Architecture for Real-Time DDoS Detection and Mitigation

The framework, as illustrated in Figure 1, is composed of various interconnected blocks that work together to detect and mitigate Distributed Denial of Service (DDoS) attacks. The

packet capture layer is responsible for capturing real-time traf-fic using WinDivert [10]. This captured traffic is sent to the traffic analysis and detection layer.

The traffic analysis and detection layer is responsible for feature extraction and statistical analysis. This layer analyzes various parameters such as packet rates, IP address activities, and protocol distribution. This analysis is done to detect any anomalies using threshold-based detection techniques [14].

The mitigation layer takes immediate action when any ma-licious traffic is detected. This is done by eliminating mali-cious packets and blocking malicious IP addresses. In addition to this, a logging and monitoring system is also incorporated. This system records all activities, which can be used for gen-erating alerts and visualizing them using a dashboard.

The framework is designed in such a way that threshold val-ues can be changed over time to improve detection accuracy.

5. RESULTS AND DISCUSSION

The proposed real-time DDoS detection and mitigation system was evaluated under simulated attack conditions by generating high-volume network traffic from multiple sources. The sys-tem was tested to analyze its ability to detect abnormal traffic patterns and respond effectively in real-time.

5.1 Performance Evaluation

Table 1: Performance Comparison of DDoS Detection Systems

Metric	Traditional	Proposed
Detection Speed	Slow	Fast
Response Time	High	Low
Packet Loss	Medium	Low
Attack Mitigation	Partial	Effective
System Stability	Moderate	High

As shown in Table 1, the proposed system significantly improves detection speed and reduces response latency compared to traditional approaches [3].

5.2 System Interface Results

Figure 1: Secure Authentication Interface

Figure 1 shows the secure authentication interface of the DDoS protection system. This login module ensures that only authorized users can access the monitoring dashboard and mitigation controls, thereby adding an additional layer of security to the system.

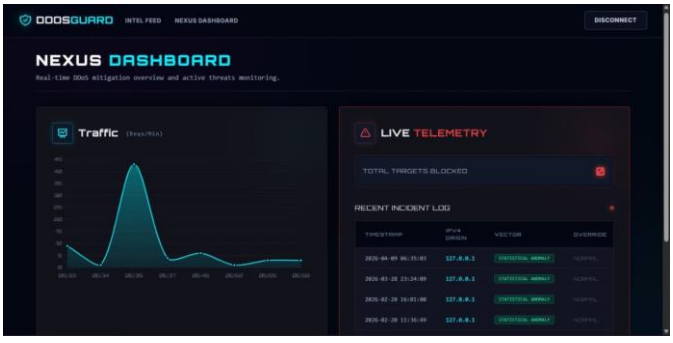

Figure 2: Real-Time Monitoring and Threat Dashboard

Figure 2 presents the real-time monitoring dashboard, which displays live traffic statistics and telemetry logs. The traffic graph helps visualize abnormal spikes in incoming re-quests, while the

incident log records detected suspicious activities for further analysis. Such real-time visualization improves rapid anomaly identification and response efficiency [2, 14].

5.3 Discussion

The experimental results demonstrate that the proposed system can effectively detect high-rate DDoS attacks with mini-mal delay. The real-time packet inspection approach ensures fast anomaly detection and immediate mitigation.

However, as discussed in prior research [11], threshold-based detection methods may struggle with low-rate dis-tributed attacks, indicating the need for adaptive or machine learning-based improvements.

6. FUTURE WORK

The scope of future work could also involve improving aspects of the system to enhance its performance and flexibility. This does not compromise its real-time detection and mitigation of high-rate DDoS attacks.

Future work could also involve incorporating machine learning-based anomaly detection techniques that can detect complex and low-rate distributed attacks that might not be detected using static threshold detection. Developing adaptive threshold detection mechanisms that can adjust detection parameters according to changing network environments could also be explored.

The incorporation of statistical detection techniques such as entropy calculations and variance analysis could also potentially improve detection accuracy. Expanding the scope of

this system to incorporate multi-layer security using cloud-based firewalls and intrusion detection systems could also be explored.

Another direction that could be explored is creating a real-time visualization dashboard that can help monitor network activities and performance. This can potentially help network administrators gain better insights.

Finally, testing this system in real-world environments could also help evaluate its performance under diverse and high-traffic network environments.

7. CONCLUSION

This paper presents a real-time DDoS detection and mitigation framework based on the analysis of packet traffic. The frame-work analyzes the real-time traffic, detects the patterns, and identifies the anomalies using a threshold-based mechanism.

Once the anomalies are detected, the mitigation process is initiated in real-time by dropping the packets and blocking the IP addresses. The proposed framework is efficient, lightweight, and doesn’t require any complicated infrastructure.

The results show the efficiency of the proposed framework in detecting the DDoS attacks in real-time, thereby providing high stability to the network. The proposed framework is efficient in mitigating the DDoS attacks without affecting the legitimate users.

The proposed framework provides a solution to enhance the security of the networks in a cost-effective way. The proposed framework has the potential to serve as a basis for developing intelligent DDoS attack mitigation systems in the future.

ACKNOWLEDGEMENT

The authors would like to express their sincere gratitude to Prof. Deepti Janjani for her valuable guidance, continuous support, and insightful suggestions throughout the development of this project. Her mentorship played a significant role in shaping the direction and quality of this research work.

The authors also thank the Department of Artificial Intelligence and Data Science at Datta Meghe College of Engineering for providing the necessary resources and environment to successfully complete this work.

Finally, the authors acknowledge the contributions of open-source tools and libraries, particularly WinDivert, which made the implementation of this system possible.

REFERENCES

[1] J. Mirkovic and P. Reiher, "A taxonomy of DDoS at-tack and DDoS defense mechanisms," ACM SIGCOMM Computer Communication Review, 2004.

[2] S. Yu, W. Zhou, R. Doss, and W. Jia, "Traceback of DDoS attacks using entropy variations," IEEE Transactions on Parallel and Distributed Systems, 2013.

[3] T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of network-based defense mechanisms against DDoS at-tacks," ACM Computing Surveys, 2007.

[4] A. Behal and K. Behal, "Cyberwar, cyberterrorism and cybercrime in the digital age," Springer, 2017.

[5] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: classification and state-of-the-art," Computer Networks, 2004.

[6] S. M. Specht and R. B. Lee, "Distributed Denial of Service: Taxonomies of attacks, tools and countermeasures," IEEE Workshop, 2004.

[7] H. Wang, D. Zhang, and K. G. Shin, "Detecting SYN flooding attacks," IEEE INFOCOM, 2002.

[8] A. Kuzmanovic and E. Knightly, "Low-rate TCP-targeted denial of service attacks," ACM SIGCOMM, 2003.

[9] M. Roesch, "Snort: Lightweight intrusion detection for networks," USENIX, 1999.

[10] WinDivert Documentation, "Windows Packet Diverting Library," Available: https://reqrypt.org/windivert.html

[11] S. Axelsson, "Intrusion detection systems: A survey and taxonomy," Technical Report, 2000.

[12] K. Hwang, M. Cai, Y. Chen, and M. Qin, "Hybrid intrusion detection with weighted signature generation," IEEE Transactions, 2007.

[13] Y. Chen, K. Hwang, and W. Ku, "Collaborative detection of DDoS attacks over multiple network domains," IEEE Transactions, 2007.

[14] A. Patcha and J. M. Park, "An overview of anomaly detection techniques," Computer Networks, 2007.