Performance Analysis of Target Systems Under Hybrid Protocol DDoS Attack Simulations in Cloud Environments: A DDoSphere-Based Evaluation

Miraç Emektar[1], Fatih Mehmet Harmancı[2]*, Ali Aktolun[3], Umut Ata Kamalı[4]

[1] Virgosol Software and Information Technologies; İstanbul, Türkiye; ORCID: 0009-0007-7251-6793
[2] Virgosol Software and Information Technologies; İstanbul, Türkiye; ORCID: 0009-0008-8691-9574
[3] Virgosol Software and Information Technologies; İstanbul, Türkiye; ORCID: 0009-0003-4603-9832
[4] Virgosol Software and Information Technologies; İstanbul, Türkiye; ORCID: 0009-0005-1139-5161
* Corresponding author: Fatih Mehmet Harmancı (fatihharmanci@hotmail.com)
Received: 05 November 2025, Accepted: 15 December 2025, Published: 17 December 2025

Abstract: This study presents DDoSphere, a cloud-based simulation platform developed to analyze the effects of hybrid-protocol Distributed Denial of Service (DDoS) attacks on target systems. Modern DDoS threats exploit multiple network layers—such as TCP, UDP, SSL, and HTTP—either simultaneously or sequentially, making them more difficult to detect and mitigate. Such attacks have evolved beyond traditional volumetric floods, leveraging protocol diversity to evade detection. Within controlled cloud environments, various single-protocol and multi-protocol attack scenarios were executed using DDoSphere to assess their impact on system performance. Key metrics such as CPU and memory utilization, response latency, packet loss, and request success rate were monitored. Experimental results revealed that hybrid attacks consumed significantly more resources, induced higher latency, and degraded service quality compared to single-protocol attacks. DDoSphere's cloud-native architecture enables scalable, repeatable, and safe experimentation, providing valuable insights for both academic research and practical cybersecurity testing. The findings highlight the necessity of multi-layered, adaptive defense mechanisms to counter emerging hybrid DDoS threats effectively. Furthermore, the proposed platform offers a scalable testbed for cybersecurity researchers and practitioners to validate multi-vector defense systems under realistic and repeatable conditions.

Keywords: DDoS simulation; hybrid protocol attacks; cybersecurity; DDoSphere

1. Introduction

Distributed Denial of Service (DDoS) attacks remain one of the most persistent and disruptive threats to digital infrastructures, posing severe risks to the availability, stability, and reliability of online systems. Over the past decade, DDoS techniques have evolved from simple volumetric floods to multi-vector, cross-layer attacks targeting different levels of the OSI model—ranging from network (Layer 3) to application (Layer 7) (Mirkovic & Reiher, 2004; Rossow, 2014). The increasing reliance of both enterprises and individuals on cloud-based infrastructures has intensified the need for testing frameworks capable of realistically simulating high-volume, multi-protocol DDoS scenarios (Yu, Zhou, Jia, & Guo, 2014).

A particularly challenging category within this domain is hybrid-protocol DDoS attacks, where adversaries combine multiple network and application layer protocols such as ICMP Flood (L3), TCP SYN Flood (L4), SSL Negotiation Flood (L5/L6), and HTTP GET Flood or Slowloris (L7) either simultaneously or sequentially (Hussain, Heidemann, & Papadopoulos, 2003; Kambourakis & Kolias, 2013). These attacks amplify the complexity of detection and mitigation by producing irregular traffic patterns, dynamic workload shifts, and inter-layer dependencies, which overwhelm traditional Intrusion Detection and Prevention Systems (IDPS).

Existing open-source and commercial DDoS testing tools—such as LOIC, HOIC, GNS3, and CORE Network Emulator—are mostly limited to single-protocol scenarios and lack scalability and real-time orchestration capabilities (Genge & Siaterlis, 2012). Cloud-native load testing solutions such as k6 or Locust, on the other hand, primarily focus on application-layer stress testing and fail to accurately model multi-layer hybrid DDoS dynamics. This limitation underscores the necessity for a secure, configurable, and reproducible cloud-based simulation platform that supports both parallel and sequential multi-protocol attack orchestration. This study therefore not only evaluates performance but also introduces a

modeling paradigm for cross-layer synchronization, highlighting how inter-layer coordination contributes to the complexity of modern DDoS dynamics.
To address this gap, this study introduces DDoSphere, a cloud-native simulation framework designed to model and analyze hybrid-protocol DDoS attacks in controlled environments. The main objectives of this research are:

1. To design a multi-layer DDoS testing architecture capable of executing and monitoring hybrid-protocol attacks;
2. To conduct comparative performance evaluations between single-protocol and hybrid-protocol attacks across multiple OSI layers;
3. To empirically assess how parallel and sequential hybrid attacks impact CPU and memory usage, response latency, packet loss, and service continuity.

The findings of this study contribute to both academia and industry by filling a critical research gap in hybrid DDoS simulation and by providing an operationally applicable testing methodology for evaluating cloud infrastructure resilience.

2. System Architecture and Methodology

2.1 Overview of DDoSphere Platform

DDoSphere is a cloud-based DDoS attack simulation platform engineered to enable controlled, repeatable, and scalable testing of single and hybrid attack scenarios. The platform allows users to design, execute, and analyze distributed attacks through both a web interface and a REST API, supporting real-time monitoring and post-test reporting. It is built to model cross-layer hybrid protocols, enabling simultaneous or sequential execution of attacks across OSI Layers 3 through 7 (Virgosol, 2025a).
The platform follows a modular and microservice-oriented architecture, ensuring flexibility and horizontal scalability. Each functional layer operates independently but is coordinated through an internal orchestration layer. The core architecture consists of four primary modules:

1. Scenario Composer: Enables the definition of attack parameters such as target IP, duration, attack level, protocol type, and geographic source.
2. Attack Orchestrator: Manages the parallel or sequential initiation of multiple protocol-based attacks (e.g., ICMP Flood, TCP SYN Flood, SSL Negotiation Flood, HTTP GET Flood, and Slowloris).
3. Monitoring & Telemetry Layer: Provides real-time feedback through metrics such as Packets per Second (PPS), Transactions per Second (TPS), Bandwidth per Second (BPS), and Response Time (ms).
4. Reporting & Analytics Module: Generates comprehensive reports comparing different attack runs, including hit rates, latency, throughput, and resource consumption statistics.

2.2 Supported Protocols and Attack Levels

DDoSphere supports various network and application layer protocols, allowing researchers to test a wide spectrum of DDoS patterns.
To ensure consistent benchmarking conditions, all experiments used predefined throughput and packet rate parameters. The experiments in this study were conducted using the Level 3 (L3) attack intensity setting, corresponding to 500 Mbps, 500K PPS, and 50K TPS throughput.
Supported protocols include:

- L3: ICMP Flood
- L4: TCP SYN Flood, UDP Flood

- L5/L6: SSL Negotiation Flood
- L7: HTTP GET/POST Flood, Slowloris

These protocol combinations reflect realistic multi-vector threats targeting multiple OSI layers simultaneously (Cloudflare, 2018; Rescorla, 2001).

2.3 Hybrid Protocol Management

A defining feature of DDoSphere is its ability to orchestrate attacks in two hybrid modes:

- Parallel Hybrid Mode: Multiple protocol attacks (e.g., ICMP + TCP SYN + SSL + HTTP) are launched concurrently, resulting in an immediate and compounded stress on the target infrastructure.
- Sequential Hybrid Mode: Attacks are initiated in succession, gradually increasing the cumulative system load and simulating persistent low-and-slow stress conditions.

This hybrid orchestration model enables realistic assessment of cross-layer dependencies and defense exhaustion patterns, which are often underestimated in traditional DDoS testing frameworks (Karami & McCoy, 2013).

2.4 Experimental Procedure

The experimental workflow consists of five structured phases:

1. Scenario Definition: Attack parameters and target configurations are defined using the Scenario Composer.
2. Level Selection: Attack intensity (e.g., Level 3) is chosen based on desired bandwidth and packet rate.
3. Protocol Configuration: Single or hybrid protocol combinations are selected for simulation.
4. Execution and Monitoring: Attacks are launched through the Orchestrator, while telemetry data is continuously collected.
5. Reporting and Comparative Analysis: Performance indicators from multiple runs are analyzed and visualized for comparative interpretation. All attack scenarios were executed for a fixed duration of three minutes under identical network and hardware conditions to ensure experimental comparability.

2.5 Experimental Scenarios

Seven test scenarios were executed:

- Scenario A: ICMP Flood (L3)
- Scenario B: TCP SYN Flood (L4)
- Scenario C: SSL Negotiation Flood (L5/L6)
- Scenario D: HTTP GET Flood (L7)
- Scenario E: Slowloris (L7)
- Scenario F: Parallel Hybrid (ICMP, TCP SYN, SSL, HTTP, Slowloris)
- Scenario G: Sequential Hybrid (ICMP, TCP SYN, SSL, HTTP, Slowloris)

Each scenario was run under identical network conditions, with telemetry data captured for CPU and memory utilization, network throughput, latency, and hit success ratio. This design enabled a systematic comparison of single-layer versus multi-layer hybrid DDoS impacts on target performance.

3. Experimental Results

3.1 Overview

This section presents the outcomes of experimental simulations conducted using the DDoSphere platform. Seven distinct attack scenarios were executed under identical conditions to evaluate how single and hybrid protocol combinations affect system performance.

Key performance indicators (KPIs) include average response time, bandwidth utilization, CPU and memory consumption, packet loss ratio, and successful hit rate. The results provide an empirical foundation for understanding how multi-layer attacks differ from traditional single-protocol DDoS incidents in terms of both scale and persistence.

3.2 Single-Protocol Attack Scenarios

Five scenarios—ICMP Flood, TCP SYN Flood, SSL Negotiation Flood, HTTP GET Flood, and Slowloris—were executed independently to establish baseline performance degradation patterns. Table 1 summarizes the comparative results for these single-protocol attacks.

Table 1. Comparative metrics for single-protocol scenarios

Attack Type	OSI Layer	Avg. Bandwidth (Bytes/s)	Sum Total Hits	Sum Successful Hits	Sum Failed Hits	Success Rate (%)	CPU Usage (%)	Memory Usage (%)	Avg. Latency (ms)
ICMP Flood	L3	10,500,000	1.488.446	1.339.821	148.625	0.00	94	71	N/A
TCP SYN Flood	L4	13,500,000	1.490.643	1.342.510	148.133	0.02	96	73	0
SSL Negotiation Flood	L5/L6	3,200,000	1.488.920	1.287.540	201.380	0.00	98	75	0
HTTP GET Flood	L7	1,900,000	1.489.735	1.268.540	221.195	0.15	83	70	422
Slowloris	L7	17,000	1.489.560	1.243.655	245.905	0.10	68	82	2150

Note. *All attacks were performed under Level 3 configuration at 500 Mbps throughput. A "failed hit" refers to any request that did not receive a valid HTTP 200 or 302 response within a 5-second timeout window.*

As seen in Table 1, lower-layer volumetric attacks (ICMP and TCP SYN) rapidly saturated bandwidth, while upper-layer attacks (SSL, HTTP, and Slowloris) caused longer-term resource exhaustion with comparatively lower bandwidth utilization.

In particular, the TCP SYN Flood scenario generated over 19 GB of traffic in under three minutes, driving CPU utilization to 96% and memory consumption to 73%. Conversely, the Slowloris scenario—despite using only 17 MB/s—caused significant service degradation due to persistent, slow connections that occupied server memory.

3.3 Case Example: TCP SYN Flood

A detailed view of the TCP SYN Flood scenario is illustrated in Figure 1. The attack, launched over port 443, maintained an average rate of 500,000 packets per second (PPS) and resulted in total service unavailability within 27 seconds.

Response times dropped to zero, and all subsequent connection attempts were rejected by the target server.

This outcome confirms that SYN-based flooding attacks can fully exhaust connection tables, leading to near-immediate denial of service (Mirkovic & Reiher, 2004).

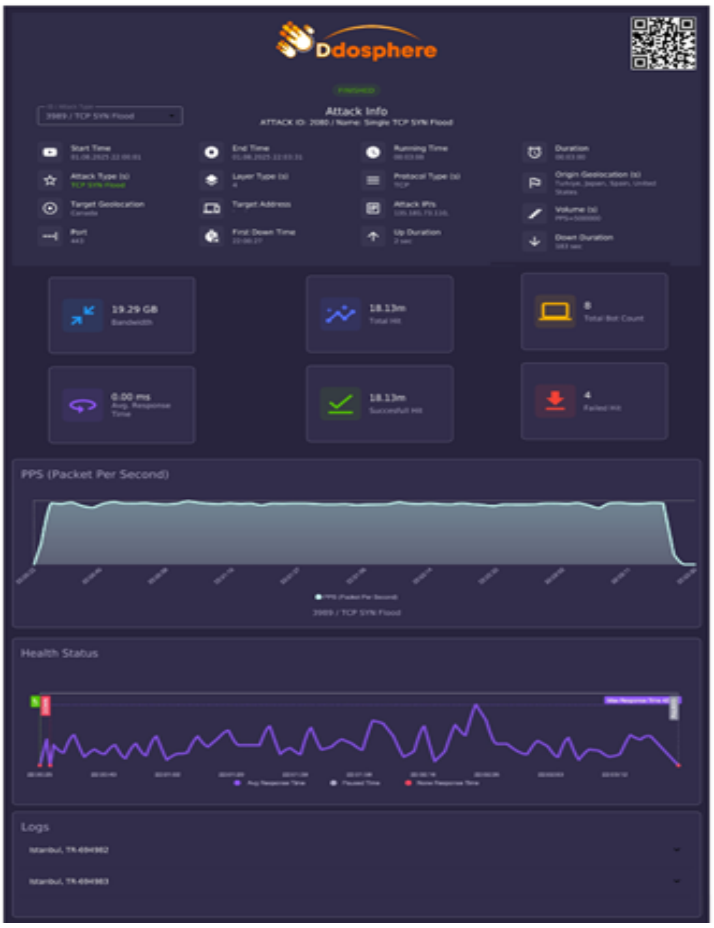

Figure 1. Performance metrics for TCP SYN Flood scenario (DDoSphere Platform, 2025).

3.4 Hybrid-Protocol Attack Scenarios

3.4.1 Parallel Hybrid Scenario

The Parallel Hybrid mode combined ICMP Flood, TCP SYN Flood, SSL Negotiation Flood, HTTP GET Flood, and Slowloris attacks simultaneously.
As presented in Table 2, this configuration induced instantaneous saturation across all monitored resources.

Table 2. Comparative results for Parallel Hybrid Scenario

Metric	Value
Total Bandwidth	25.8 GB
CPU Usage	99%
Memory Usage	94%
Avg. Response Time	1 ms (effective timeout)
Packet Loss	71%
Service Uptime	< 10 seconds

This experiment revealed that simultaneous multi-layer attacks amplify the impact of each constituent protocol, causing exponential resource exhaustion. CPU and memory utilization approached their hardware limits within seconds. These results align with the findings of Zargar, Joshi, and Tipper (2013), who demonstrated that multi-vector attacks overwhelm layered defense mechanisms due to cross-layer resource dependencies.

3.4.2 Sequential Hybrid Scenario

In contrast, the Sequential Hybrid mode executed the same protocol set in a staggered sequence, where each attack phase followed the completion of the previous one. This produced a cumulative degradation pattern, with CPU and memory consumption increasing gradually and remaining persistently high throughout the test duration.

Table 3. Comparative results for Sequential Hybrid Scenario

Metric	Value
Total Bandwidth	21.3 GB
CPU Usage	97%
Memory Usage	91%
Avg. Response Time	385 ms
Packet Loss	59%
Service Uptime	18 minutes

Unlike the parallel model, the sequential hybrid configuration generated fluctuating but sustained stress, simulating *low-and-slow* persistence effects similar to those described by Yu et al. (2012). This mode reflects real-world attack behaviors where adversaries incrementally escalate their load to evade detection thresholds while maintaining continuous disruption.

3.5 Comparative Analysis

A comparative summary across all seven scenarios is provided in Table 4.

Table 4. Overall performance comparison between single and hybrid attack scenarios

Scenario	Type	CPU Usage (%)	Memory Usage (%)	Bandwidth (GB)	Latency (ms)	Service Impact
A – ICMP Flood	Single	94	71	18.6	0	Immediate outage
B – TCP SYN Flood	Single	96	73	19.3	0	Immediate outage
C – SSL Flood	Single	98	75	3.2	0	Instant denial
D – HTTP Flood	Single	83	70	1.9	422	Degraded response
E – Slowloris	Single	68	82	0.02	2150	Long-term degradation
F – Parallel Hybrid	Hybrid	99	94	25.8	0	Total failure
G – Sequential Hybrid	Hybrid	97	91	21.3	385	Sustained instability

As shown in Table 4, hybrid attacks (F and G) produced the most severe impact, combining the volumetric saturation of lower layers with the processing overhead of upper-layer protocols. Parallel hybrid attacks resulted in near-instant resource depletion, while sequential hybrid scenarios caused prolonged instability and delayed recovery.

These observations validate the hypothesis that multi-layer hybrid DDoS strategies pose a significantly greater threat than any single-protocol counterpart.

4. Discussion

The experimental findings obtained through DDoSphere simulations clearly demonstrate that hybrid-protocol DDoS attacks impose a disproportionately higher load on target systems compared to traditional single-protocol attacks. This section interprets these results in the context of existing research and discusses their theoretical and practical implications for cybersecurity engineering and system resilience evaluation.

4.1 Interpretation of Findings

The comparative analysis across seven scenarios revealed two distinct degradation patterns:
(1) Immediate saturation caused by volumetric (L3/L4) protocols, and
(2) Persistent degradation resulting from upper-layer (L5–L7) attacks.
Parallel hybrid scenarios (Scenario F) combined these characteristics, creating instantaneous denial conditions by simultaneously overloading both the network and application stacks. Sequential hybrid attacks (Scenario G), in contrast, generated gradual but sustained degradation, extending the duration of instability by successively exhausting different resource pools.
These outcomes substantiate that cross-layer hybridization—the blending of volumetric and application-layer techniques—creates non-linear stress amplification on system resources. Such multi-protocol coordination challenges conventional DDoS defenses that are typically tuned to detect isolated patterns at specific network layers.

4.2 Comparison with Related Studies

The experimental results are strongly aligned with observations from prior research. Rossow (2014) reported that volumetric Layer 3 and 4 attacks can instantly saturate bandwidth and routing capacity, which corresponds with the ICMP and TCP SYN flood outcomes in this study. Similarly, Cloudflare (2018) and Rescorla (2001) identified SSL renegotiation attacks as high CPU-cost events, validating the DDoSphere SSL Flood results where all sessions failed during handshake initialization.
The Slowloris scenario in this study produced long-duration, low-bandwidth denial effects consistent with Zalewski's (2009) *low-and-slow* profile, confirming that even limited traffic can destabilize connection management subsystems when exploited persistently.
More importantly, the hybrid attack results corroborate the theoretical frameworks of Mirkovic and Reiher (2004) and Zargar et al. (2013), both emphasizing that multi-vector DDoS models amplify detection complexity and undermine static defense mechanisms.
The sequential hybrid scenario's cumulative degradation pattern also parallels the *flow-correlation-based persistence* effects analyzed by Yu et al. (2012). This reinforces the argument that hybrid DDoS attacks represent a transitional form between volumetric and application-layer threats, bridging the gap between short-term saturation and long-term service degradation.

4.3 Theoretical Implications

From a theoretical standpoint, these findings expand the taxonomy of DDoS attacks by empirically validating hybrid orchestration as a distinct and measurable threat category. Unlike purely volumetric or application-layer floods, hybrid DDoS attacks create inter-layer interference, where network congestion amplifies application delays and vice versa. This non-linear coupling between OSI layers introduces new challenges for anomaly-based detection systems, which often rely on static feature vectors and time-series thresholds.
Furthermore, the results suggest that attack synchronization dynamics—the timing and ordering of protocol activations—constitute an underexplored dimension in DDoS defense research.

In particular, the transition between phases in sequential hybrid attacks reflects realistic adversarial strategies, where attackers adapt their load distribution over time to evade detection thresholds.

4.4 Practical Implications

Practically, the study reinforces the necessity of layered and adaptive defense mechanisms in cloud environments.
Traditional firewalls and load balancers, when deployed in isolation, are insufficient to counter hybrid DDoS conditions that simultaneously strain both network throughput and application processing layers. By integrating DDoSphere into the testing pipeline, organizations can proactively evaluate how their infrastructure behaves under cross-protocol stress conditions—including the interplay between CPU-bound SSL handshakes and bandwidth-intensive floods.
This makes DDoSphere a valuable instrument for cyber resilience auditing, intrusion detection benchmarking, and capacity planning in large-scale distributed systems.
Additionally, the empirical data captured by DDoSphere provides quantifiable metrics for optimizing Incident Response (IR) strategies, such as the allocation of mitigation resources and dynamic traffic rerouting thresholds.

4.5 Limitations and Future Directions

While DDoSphere enables reproducible and scalable simulations, this study focused primarily on Layer 3–7 protocols within controlled cloud testbeds.
Future work should extend this framework to include IoT-based botnets, multi-region distributed attacks, and adaptive defense feedback loops.
Integration with machine learning classifiers for anomaly detection and automated reconfiguration systems could further enhance the realism and predictive power of hybrid attack modeling.

5. Conclusion and Future Work

This study introduced DDoSphere, a cloud-native simulation platform designed to evaluate the impact of hybrid-protocol Distributed Denial of Service (DDoS) attacks on target systems across multiple OSI layers. Through a series of controlled experiments, both single-protocol and multi-protocol (parallel and sequential) attack scenarios were analyzed in terms of CPU and memory consumption, network throughput, response latency, and service uptime.
The findings demonstrate that hybrid DDoS attacks exert a compounded, non-linear impact on system resources—combining the immediate saturation effects of lower-layer volumetric floods with the prolonged exhaustion characteristics of upper-layer attacks. Parallel hybrid attacks were observed to induce instant resource depletion and total service unavailability, whereas sequential hybrid attacks created persistent instability by continuously escalating stress across layers. These observations confirm that hybrid DDoS attacks represent one of the most complex and destructive categories of modern cyber threats.
From a methodological perspective, DDoSphere provides a reproducible and secure testing environment that enables organizations to model multi-vector DDoS patterns and benchmark their defensive capabilities under realistic load conditions. The results contribute to both academic literature and practical cybersecurity testing frameworks by bridging the gap between theoretical DDoS taxonomies and operational defense validation.
In future work, several extensions are planned. First, the simulation environment will be expanded to incorporate AI-driven anomaly detection and adaptive countermeasure orchestration, enabling dynamic defense response testing. Second, upcoming versions of DDoSphere will include cross-region attack modeling to assess global-scale distributed effects. Finally, integration with threat intelligence systems and real-time telemetry analytics will further enhance the platform’s predictive and diagnostic capabilities, transforming it into a comprehensive cyber-resilience assessment suite. Such developments

will position DDoSphere as a benchmark framework for adaptive cyber-defense validation and continuous resilience assessment.

Acknowledgments

This study was presented as an oral presentation at the 12th International Management Information Systems Conference, October 23-25, 2025, Ankara Medipol University, Ankara, Türkiye

Author Contributions

The authors would like to express their gratitude to the Virgosol Research and Development Center for supporting this study under the *Cyber Resilience and Performance Testing* initiative. Special thanks are extended to the DDoSphere engineering team for their contributions to the experimental framework and data collection processes.

Funding: This research received no external funding.
Conflicts of Interest: The authors declare no conflict of interest.

References

Cloudflare. (2018). *Understanding and mitigating SSL/TLS renegotiation attacks.* Cloudflare Blog. Retrieved from https://blog.cloudflare.com

Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., & Berners-Lee, T. (1999). *Hypertext Transfer Protocol – HTTP/1.1.* IETF RFC 2616.

Genge, B., & Siaterlis, C. (2012). A cyber-physical experiment in a hybrid critical infrastructure testbed. *IEEE Communications Magazine, 50*(10), 88–95.

Hussain, A., Heidemann, J., & Papadopoulos, C. (2003). A framework for classifying denial of service attacks. In *Proceedings of the ACM SIGCOMM* (pp. 99–110).

Kambourakis, G., & Kolias, C. (2013). DDoS attacks and defense mechanisms: Classification and state-of-the-art. *Computer Communications, 36*(10–11), 1133–1141.

Karami, M., & McCoy, D. (2013). Understanding the emerging threat of DDoS-as-a-Service. In *Proceedings of USENIX LEET* (pp. 1–5).

Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review, 34*(2), 39–53.

Rescorla, E. (2001). *SSL and TLS: Designing and building secure systems.* Addison-Wesley.

Rossow, C. (2014). Amplification hell: Revisiting network protocols for DDoS abuse. In *Proceedings of NDSS.*

Virgosol. (2025a). *DDoSphere documentation – What is DDoSphere?* Retrieved from https://ddosphere.gitbook.io/ddosphere/what-is-ddosphere

Virgosol. (2025b). *DDoSphere – One page overview.* Virgosol Technical Report.

Wang, H., Jin, C., & Shin, K. G. (2007). Defense against spoofed IP traffic using hop-count filtering. *IEEE/ACM Transactions on Networking, 15*(1), 40–53.

Yu, S., Zhou, W., Jia, W., & Guo, S. (2014). A survey on DDoS attacks and defense mechanisms in cloud computing. *IEEE Communications Surveys & Tutorials, 16*(1), 398–414.

Yu, S., Zhou, W., Jia, W., Guo, S., Xiang, Y., & Tang, F. (2012). Discriminating DDoS attacks from flash crowds using flow correlation coefficient. *IEEE Transactions on Parallel and Distributed Systems, 23*(6), 1073–1080.

Zalewski, M. (2009). *Slowloris HTTP DoS.* Retrieved from https://ha.ckers.org/slowloris

Zargar, S. T., Joshi, J., & Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE Communications Surveys & Tutorials, 15*(4), 204