alpha
Journal of Engineering and Applied Sciences
(AJEAS)
e-ISSN: 3023-6002

Alfa Mühendislik ve Uygulamalı Bilimler Dergisi
(2024) 3/1: 35 – 50

Araştırma Makalesi

DOI: 10.70988/ajeas.1628985

Gönderi (Received): 29/01/2024

Kabul (Accepted): 22/03/2025

Yayın (Published): 30/04/2025

Dağıtık Siber Saldırıların İnternet Hizmetlerinin Kullanılabilirliği Üzerindeki Etkisi: DDoSphere ile Deneysel Bir Analiz

Doğukan ÖZTÜRK [a, *], Ali AKTOLUN [a], Miraç EMEKTAR [a], Fatih Mehmet HARMANCI [a]

[a] Virgosol Bilişim ve Yazılım Çözümleri A.Ş, Yıldız Teknik Üniversitesi, Yıldız Teknopark, İstanbul,TÜRKİYE
* Sorumlu yazar e-mail adresi: fatihharmanci@hotmail.com

Özet

Bu araştırma, farklı coğrafi konumlardan kaynaklanan yoğun trafiği kullanarak sistemleri çökerten siber saldırılar olan DDoS saldırılarının, ağ performansını nasıl etkilediğini incelemeyi amaçlamıştır. Volumetrik, protokol ve uygulama katmanındaki DDoS saldırılarının, ağ üzerindeki etkileri simülasyonlarla incelenmiş ve bu saldırıların sistemlerin işlem gücünü ve bant genişliğini nasıl tükettiği detaylı olarak analiz edilmiştir. Özellikle çoklu kaynaklı saldırıların, tespit ve savunma sistemlerini zorlaması üzerine odaklanan bu çalışma, Ddosphere simülasyon aracıyla desteklenmiştir. Elde edilen sonuçlar, ağ yöneticileri ve siber güvenlik uzmanlarına, ağ performansını artırmak ve DDoS saldırılarına karşı daha etkili savunma stratejileri geliştirmek için değerli bilgiler sunmaktadır. Bu çalışma, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu'nun desteklediği "DDOS Tabanlı Siber Saldırı Test Modülü" projesi kapsamında Virgosol tarafından yürütülmüştür.

Anahtar kelimeler: *DDoS saldırıları, Ağ performansı, Siber güvenlik, Ddosphere, Çoklu konumlu saldırılar, Simülasyon tabanlı analiz, Savunma stratejileri*

The Impact of Distributed Cyberattacks on the Availability of Internet Services: An Empirical Analysis with DDoSphere

Abstract

This research aims to examine how DDoS attacks, which are cyberattacks that use heavy traffic from different geographical locations to disrupt systems, affect network performance. The impact of DDoS attacks at the volumetric, protocol, and application layers on networks was analyzed through simulations, and the way these attacks consume system processing power and bandwidth thoroughly studied. This study specifically focuses on the challenges posed by multi-sourced attacks to detection and defense mechanisms, and is supported by the Ddosphere simulation tool. The findings provide valuable insights for network administrators and cybersecurity experts to enhance network performance and to develop more effective defense strategies against DDoS attacks. This study was conducted by Virgosol within the scope of the "DDoS-Based Cyberattack Test Module" project, and it was supported by the Scientific and Technological Research Council of Turkey (TÜBİTAK)

Keywords: *DDoS attacks, Network performance, CyberSecurity, Ddosphere, Multi-location attacks, Simulation-based analysis, Defense strategies*

Citation: Authors, “Dağıtık Siber Saldırıların İnternet Hizmetlerinin Kullanılabilirliği Üzerindeki Etkisi: DDoSphere ile Deneysel Bir Analiz”, AJEAS. (2025) 3(1): 35-50. http://dx.doi.org/10.70988/ajeas.1628985

1. Giriş *(Introduction)*

İnternet, dünya çapında yüz milyonlarca bilgisayarı birbirine bağlayan ve farklı donanım ve yazılım platformlarında çalışan devasa bir ağdır. İnternet, hem kişisel hem de kurumsal ihtiyaçları karşılayarak önemli hizmetler sunar. Ancak, bu ağ üzerinden sağlanan bağlantılar, kötü niyetli kullanıcıların kaynakları kötüye kullanmasına ve belirli sitelere yönelik hizmet reddi (DoS) saldırıları gerçekleştirmesine olanak tanır.

Hizmet reddi saldırısı, kötü niyetli bir kullanıcının internetin bağlantı olanaklarını kullanarak bir sitenin hizmetlerini engellemeye çalıştığı bir durumdur. Genellikle bu, hedef siteye aşırı miktarda istek gönderilerek gerçekleştirilir [1]. Bu tür saldırılar, tek bir kaynaktan gelebileceği gibi, birçok bilgisayarın koordine bir şekilde hedefe istek yağmuru göndermesiyle de yapılabilir. Bu ikinci tür saldırıya, dağıtık hizmet reddi (DDoS) saldırısı denir.

İnternet ortamı geniş bilgi ve araçlara ev sahipliği yapmaktadır, kötü niyetli saldırılar düzenlemeyi otomatikleştiren gelişmiş saldırı araçlarını da barındırır ve ayrıntılı kullanım talimatları sayesinde, amatörler bile bu araçları kolaylıkla ve etkili bir şekilde kullanabilir [1].

Hizmet reddi saldırıları her yıl önemli finansal zararlara neden olur ve bu nedenle, bu tür saldırıları hızla tespit edip yanıt verecek tekniklerin geliştirilmesi büyük önem taşır. Bu durumun çarpıcı bir örneği, ABD merkezli bulut tabanlı bir Git deposu barındırma hizmeti sunan GitHub'ın tarihin en büyük DDoS saldırılarından birine maruz kalmasıyla yaşandı. Bu saldırıda, bilinmeyen hackerlar platforma 1,35 Tbps'lik devasa bir trafik yükleyerek GitHub'ı çevrimdışı bırakmaya çalıştı. Sonuç olarak, ABD'nin geniş bir bölgesindeki önemli web siteleri saatlerce hizmet dışı kaldı [2].

Günümüzde DDoS saldırıları hem yöntem hem de şiddet bakımından yeni boyutlara ulaşmış durumda ve mevcut eğilimler, benzer saldırıların gelecekte de gerçekleşebileceğini göstermektedir. Siber güvenlik, kuruluşların siber savaşta galip gelebilmesi için kritik bir rol oynar. İşletmeler, siber güvenlik önlemlerini diğer operasyonel süreçlerle aynı öncelikte değerlendirmediğinde, yalnızca bir sonraki DDoS saldırısının hedefi olma riskiyle kalmazlar; aynı zamanda büyük çapta itibar kaybı ve mali zararlara da maruz kalabilirler.

Hizmet reddi saldırıları, kaynaklarına göre iki ana gruba ayrılabilir: bunlar tek kaynaklı ve çok kaynaklı saldırılardır. Tek kaynaklı DoS saldırıları, gerçekten de tek bir cihaz veya IP adresinden gelen zararlı trafikle sistemleri işlevsiz hale getirmeye çalışır. Bu tür saldırılarda, saldırgan tüm trafiği belirli bir noktadan gönderir, bu da saldırının kaynağını tespit etmeyi ve engellemeyi nispeten daha kolay hale getirebilir.

Çok kaynaklı saldırılar ise genellikle farklı coğrafi bölgelerden gelen trafiği içerir. Bu tür saldırılar, saldırganların farklı fiziksel lokasyonlardan aynı anda saldırı başlatmasıyla gerçekleştirilir. Bu, saldırının tespit edilmesini ve önlenmesini daha da zorlaştırır, çünkü saldırı trafiği farklı ülkelerden veya bölgelerden gelebilir. Bu da saldırıya karşı alınacak önlemleri karmaşık hale getirir.

Bu çalışmanın amacı, farklı coğrafi konumlardan gelen dağıtılmış hizmet reddi (DDoS) saldırılarının ağ performansı üzerindeki etkilerini incelemektir. Çalışmada, volumetrik saldırılar (örneğin, UDP Flood), protokol saldırıları (örneğin, SYN Flood) ve uygulama katmanı saldırıları (örneğin, HTTP Flood) gibi farklı DDoS saldırı türlerinin ağ üzerindeki etkileri analiz edilecektir. Bu saldırıların, gecikme süresi, paket kaybı ve bant genişliği kullanımı gibi kritik ağ performans metrikleri üzerindeki etkileri değerlendirilecektir. Ayrıca, Ddosphere simülasyon aracı kullanılarak tek lokasyondan ve çoklu lokasyonlardan gerçekleştirilen saldırıların karşılaştırmalı analizi yapılacak, çoklu kaynaklı

saldırıların tespit ve savunma sistemleri üzerindeki etkileri detaylı olarak incelenecektir. Çalışmanın amacı, çoklu lokasyonlardan gelen dağıtılmış hizmet reddi (DDoS) saldırılarının ağ performansı üzerindeki etkilerini incelemektir.

Çalışmamızda öncelikle, DDoS saldırılarının temel prensiplerini ve türlerini ele alacağız. Ardından tek lokasyondan ve çoklu lokasyonlardan gelen saldırıların özelliklerini ve bu saldırıların ağ üzerindeki spesifik etkilerini analiz edeceğiz. Bu bağlamda, Ddosphere ürününden faydalanarak tek lokasyondan ve çoklu lokasyonlardan gerçekleştirilen saldırıların ağ performansı üzerindeki farklarını simüle edecek ve bu simülasyonlar üzerinden performans değerlendirmeleri yapacağız. Ddosphere, saldırıları canlı olarak izlememizi, hedef sistemin performansını analiz etmemizi ve bu analizleri detaylı raporlarla sunmamızı sağlayan gelişmiş bir simülasyon aracıdır.

Bu çalışma, siber güvenlik uzmanları, ağ yöneticileri ve işletmeler için tek lokasyon ve çoklu lokasyonlardan gelen DDoS saldırılarına karşı daha bilinçli ve hazırlıklı olmalarına yardımcı olmayı amaçlamaktadır. Ddosphere kullanarak gerçekleştirilen simülasyonlar, farklı saldırı senaryolarının ağ performansını nasıl etkilediğini canlı olarak gözlemleme ve analiz etme imkânı sunacak, bu da savunma stratejilerinin etkinliğini artırmak için kritik veriler sağlayacaktır.

Sonuç olarak, çalışmamız, ağ performansını optimize etmek ve DDoS saldırılarına karşı etkili savunma mekanizmaları geliştirmek için gerekli olan bilgileri ve analizleri sunarak, siber güvenlik alanında önemli bir katkı sağlamayı hedeflemektedir.

2. DDoS Saldırısı *(DDoS Attack)*

Bu bölümde, DDoS saldırılarının türleri, gerçekleştirmek için kullanılan yöntemler, tarihsel gelişimi ve ağ performansı üzerindeki etkileri incelenecektir.

2.1. DDoS Saldırılarının Tarihsel Gelişimi *(The Historical Development of DDoS Attacks)*

Dağıtılmış Hizmet Reddi (DDoS) saldırıları, internetin yaygınlaşmasıyla birlikte evrim geçirmiş ve giderek daha karmaşık ve etkili hale gelmiştir. İlk basit saldırılardan günümüzün büyük ölçekli botnet destekli saldırılarına kadar DDoS'un gelişimi aşağıda detaylandırılmaktadır (Tablo 1).

2.1.1. 1990'lar: DDoS kavramının ortaya çıkışı *(The 1990s: The emergence of the DDoS concept)*

DDoS saldırılarının kökeni 1990'lı yıllara dayanmaktadır. İlk örneklerden biri, 1999 yılında "Trinoo" adlı bir saldırı aracıyla gerçekleştirilen saldırıdır [3]. Trinoo, yüzlerce bilgisayardan gelen yoğun trafikle hedef sunucuları devre dışı bırakmayı amaçlayan bir saldırı türüydü. Benzer şekilde, TFN (Tribe Flood Network) ve Stacheldraht gibi saldırı araçları, DDoS saldırılarının ilk nesil araçları arasında yer aldı [4].

2.1.2. 2000'ler: İlk büyük ölçekli DDoS saldırıları *(The 2000s: The first large-scale DDoS attacks)*

2000'li yılların başında, DDoS saldırıları geniş çapta zarar vermeye başladı. Özellikle Şubat 2000'de, bir genç hacker olan Mafiaboy, Yahoo, CNN, Amazon ve eBay gibi büyük sitelere koordineli DDoS saldırıları düzenleyerek hizmetlerini kesintiye uğrattı [5]. Bu saldırılar, DDoS'un internet altyapısını tehdit edebileceğini açıkça gösterdi.

2003 yılında, SQL Slammer ve Blaster solucanları, sistem açıklarını kullanarak yaygın DDoS saldırıları gerçekleştirdi [6]. Bu saldırılar, bir sistemdeki zafiyetin kullanılarak dünya genelindeki birçok sunucunun devre dışı bırakılabileceğini kanıtladı (Tablo 1).

Tablo 1. Büyük ölçekli DDoS saldırıları ***(Large-Scale DDoS Attacks)***

Yıl	Saldırı	Öne Çıkan Noktalar
1999	Trinoo, TFN, Stacheldraht	İlk DDoS saldırıları [3]
2000	Mafiaboy Saldırıları	Yahoo, Amazon ve CNN gibi büyük siteler hedef alındı [5]
2003	SQL Slammer	Worm tabanlı saldırılar başladı [6]
2013	Spamhaus DNS Amplifikasyon	300 Gbps saldırı kapasitesine ulaşıldı [7]
2016	Mirai Botnet	IoT cihazları hedef alındı, 600 Gbps saldırılar [8]
2018	GitHub Saldırısı	1.35 Tbps ile en büyük saldırılardan biri gerçekleşti [9]
2020	AWS 2.3 Tbps Saldırısı	En büyük volumetrik saldırı [10]
2022	Cloudflare & Azure Saldırıları	26 milyon RPS'ye ulaşan HTTP Flood saldırıları [11]
2023+	AI Destekli Botnetler	Yapay zeka kullanılarak daha sofistike saldırılar düzenlenmekte [12]

2.1.3. 2010'lar: Botnet destekli büyük ölçekli saldırılar *(The 2010s: Large-scale botnet-driven attacks)*

2010'lu yıllar, botnetlerin yükselişi ile DDoS saldırılarında büyük bir değişime sahne oldu.

- 2012 - 2014 Cloudflare ve Spamhaus Saldırıları: 2013 yılında, Spamhaus adlı bir anti-spam organizasyonu, 300 Gbps'yi aşan bir DDoS saldırısına maruz kaldı. Bu saldırı, dönemin en büyük DNS Amplifikasyon saldırılarından biri olarak kaydedildi [7].
- 2016 Mirai Botnet: IoT (Nesnelerin İnterneti) cihazlarını ele geçirerek 600 Gbps büyüklüğünde saldırılar gerçekleştiren Mirai botneti, Dyn DNS, OVH ve KrebsOnSecurity gibi büyük hedeflere saldırarak internetin büyük bir bölümünü etkiledi [8].
- 2018 GitHub Saldırısı: GitHub, 1.35 Tbps büyüklüğünde bir DDoS saldırısına maruz kalarak en büyük saldırılardan birine tanık oldu [9].

2.1.4. 2020 ve Sonrası: Rekor kıran DDoS saldırıları *(2020 and Beyond: Record-breaking DDoS attacks)*

Son yıllarda DDoS saldırıları daha büyük ve sofistike hale gelmiştir.

- 2020 AWS'ye Yönelik 2.3 Tbps'lik Saldırı: Amazon Web Services (AWS), 2.3 Tbps hızında bir saldırıya maruz kalarak tarihin en büyük DDoS saldırılarından birini yaşadı [10].
- 2022 Cloudflare ve Microsoft Azure'a Yönelik Saldırılar: Cloudflare ve Microsoft Azure gibi büyük bulut sağlayıcıları, saniyede 26 milyon istek seviyesine ulaşan HTTP Flood saldırılarıyla hedef alındı [11].
- 2023 - 2024 Yapay Zeka Destekli Saldırılar: Son dönemde, saldırganlar yapay zeka (AI) destekli botnetler ile daha karmaşık DDoS saldırıları düzenlemektedir [12]. Ayrıca, Web3 ve blok zinciri altyapılarına yönelik DDoS saldırıları da artış göstermektedir [13].

DDoS saldırıları, basit tek noktadan yapılan saldırılardan gelişmiş botnet ve yapay zeka destekli koordineli saldırılara evrilmiştir. Siber güvenlik önlemleri gelişse de, saldırganlar da yeni teknikler geliştirerek savunma sistemlerini aşmaya çalışmaktadır. Bu nedenle, gelecekte otomatik tespit sistemleri, yapay zeka destekli güvenlik çözümleri ve proaktif savunma mekanizmaları daha kritik hale gelecektir.

2.2. DDoS Saldırı Türleri ve Yöntemleri *(Types and Methods of DDoS Attacks)*

DDoS saldırıları, farklı teknikler kullanarak çeşitli katmanlarda gerçekleştirilir ve genel olarak üç ana türde incelenir: Volumetrik saldırılar, protokol saldırıları ve uygulama katmanı saldırıları.

2.2.1. Volumetrik saldırılar *(Volumetric attacks)*

Volumetrik saldırılar, hedefin bant genişliğini tüketerek ağ trafiğini tıkayan saldırılardır. Bu saldırılar, büyük miktarda veri trafiği göndererek hedefin ağ altyapısını boğar. Volümetrik saldırılardan biri olan UDP Flood saldırısında, UDP protokolü kullanılarak rastgele portlara büyük miktarda veri paketi gönderilir ve hedef sistem bu paketlere yanıt vermek zorunda kalarak kaynaklarını tüketir [14]. ICMP Flood saldırısında ise hedefe büyük miktarda ICMP ECHO REQUEST paketleri gönderilir. Hedef, bu paketlere yanıt vermek zorunda kalarak bant genişliğini ve işlem kaynaklarını tüketir [15].

2.2.2. Protokol saldırıları *(Protocol attacks)*

Protokol saldırıları, ağ katmanındaki zafiyetleri hedef alır ve hedefin kaynaklarını tüketerek hizmetlerin aksamasına yol açar. Protokol Saldırılarından SYN Flood saldırısında; TCP bağlantı kurulumu sırasında SYN paketleri gönderilir, ancak bağlantı tamamlanmaz. Bu durum, hedef sistemde yarım kalmış bağlantıların birikmesine neden olur ve sistemin kaynaklarını tüketir [16]. Smurf Attackta ise saldırgan, hedefin IP adresini sahte bir şekilde kaynak IP olarak göstererek ICMP, ECHO, REQUEST paketlerini geniş bir ağa gönderir. Ağdaki cihazlar, hedefe yanıt gönderir ve bu da hedefin bant genişliğini aşırı yükler [17].

2.2.3. Uygulama katmanı saldırıları *(Application layer attacks)*

Uygulama katmanı saldırıları, hedefin uygulama katmanında bulunan zafiyetleri kullanarak hizmetleri aksatmayı amaçlar. Bu saldırılar, genellikle daha az bant genişliği kullanarak yüksek etki yaratır. Uygulama Katmanı saldırılarından HTTP Flood saldırısında HTTP protokolü kullanılarak hedef web sunucusuna büyük miktarda istek gönderilir. Bu, sunucunun kaynaklarını tüketir ve hizmet vermesini engeller [18]. Slowloris saldırısında Saldırgan, hedef web sunucusuna çok sayıda yarım kalmış HTTP bağlantısı açar. Bu, sunucunun kaynaklarını tüketir ve yeni bağlantıları kabul etmesini engeller [19].

2.3. DDoS Saldırıları İçin Kullanılan Araçlar ve Teknikler *(Tools and Techniques Used for DDoS Attacks)*

DDoS saldırıları için kullanılan çeşitli araçlar ve teknikler bulunmaktadır. Bu bölümde, en yaygın ve etkili DDoS saldırı yöntemlerinden bazıları incelenecektir. Bu araç ve teknikler, saldırganların hedef sistemleri etkisiz hale getirmek için kullandıkları temel yöntemleri oluşturur.

2.3.1. Botnetler *(Botnets)*

Botnetler, zararlı yazılımlarla ele geçirilmiş bilgisayar ağlarıdır. Saldırganlar, bu bilgisayarları koordine ederek hedefe büyük miktarda trafik gönderir. IoT cihazlarını hedef alarak, bu cihazları ele geçirir ve geniş çaplı DDoS saldırıları gerçekleştirir. Mirai botneti, 2016 yılında Dyn DNS hizmetine yapılan saldırıda kullanılmıştır [20].

2.3.2. Amplifikasyon teknikleri *(Amplification techniques)*

Amplifikasyon teknikleri, küçük bir istek göndererek büyük bir yanıt alınmasını sağlar. DNS Amplifikasyon saldırılarında; saldırgan, sahte IP adresiyle DNS sunucularına küçük bir istek gönderir. DNS sunucuları, bu isteğe büyük yanıtlar vererek hedefi aşırı yükler [21]. NTP (Network Time Protocol) amplifikasyon saldırıları, küçük bir istek göndererek büyük bir yanıt alınmasını sağlayan bir saldırı türüdür. Saldırgan, NTP sunucusuna "MONLIST" komutu içeren küçük bir istek gönderir. Bu komut, NTP sunucusunun son 600 istemci IP adresini döndüren bir yanıt oluşturmasına neden olur. Gönderilen MONLIST isteği yaklaşık 64 bayt iken, yanıt paketleri toplamda 100'den fazla 482 baytlık yanıt paketine dönüşebilir. Bu da yaklaşık 1:200 oranında bir amplifikasyon sağlar [22].

2.3.3. Yönlendirilmiş Saldırılar *(Reflected Attacks)*

Yönlendirilmiş saldırılar, saldırganın hedefe doğrudan saldırmak yerine, üçüncü taraf bir sunucuya sahte bir istek göndererek hedefe yanıtın iletilmesini sağlar. DNS yönlendirilmiş saldırılarda; saldırgan, sahte IP adresiyle DNS sunucularına istek gönderir. Sunucular, hedef IP'ye yanıt gönderir ve hedefi aşırı yükler [23]. NTP yönledirilmiş saldırılarda; saldırgan, sahte IP adresiyle NTP sunucularına istek gönderir. Sunucular, hedef IP'ye büyük yanıtlar gönderir ve hedefi aşırı yükler [24].

2.4. DDoS Saldırılarının Ağ Performansı Üzerindeki Teknik Etkileri *(The Technical Effects of DDoS Attacks on Network Performance)*

DDoS saldırıları, ağ performansını ciddi şekilde etkileyebilir. Bu etkiler arasında ağ gecikmeleri, paket kaybı, bant genişliği tükenmesi ve hizmet kesintileri yer alır.

2.4.1. Ağ Gecikmeleri *(Latency)*

DDoS saldırıları, ağdaki veri paketlerinin hedefe ulaşma süresini artırarak ağ gecikmelerine neden olur. Bu gecikmeler, ağ cihazlarının aşırı yüklenmesi ve bekleme sürelerinin artması sonucu oluşur.

Queueing Delay (Kuyruk Gecikmesi). Ağ cihazları, büyük miktarda gelen trafiği işleyemez hale gelir ve paketler işlenmek üzere kuyrukta bekler. Bu durum, veri iletiminde gecikmelere neden olur [25].

2.4.2. Paket Kaybı *(Packet Loss)*

Aşırı trafik, ağ cihazlarının kapasitesini aştığında, cihazlar daha fazla paket işleyemez hale gelir ve bu da paket kaybına neden olur.

Buffer Overflow (Tampon Taşması). Yönlendirici tamponları dolduğunda, yeni gelen paketler düşürülür ve paket kaybı yaşanır. Bu durum, saldırı sırasında ağın genel performansını ve hizmet kalitesini düşürür.

2.4.3. Bant Genişliği Tükenmesi *(Bandwidth Exhaustion)*

Volumetrik saldırılar, ağın tüm bant genişliğini tüketerek diğer trafiğin geçişine engel olur.

2.4.4. Bağlantı Doygunluğu *(Link Saturation)*

Saldırı trafiği, ağ bağlantılarının taşıma kapasitesini aşar ve bağlantılar tamamen dolar. Bu, saldırı trafiği dışında hiçbir trafiğin geçememesi anlamına gelir. Bu da hizmet kesintilerine ve kullanıcıların hizmete erişememesine neden olabilir [26].

3. Yöntem *(Method)*

Bu çalışmanın amacı, farklı lokasyonlardan gerçekleştirilen DDoS saldırılarının ağ performansına etkilerini gözlemlemek ve Ddosphere aracının bu konudaki yeteneklerini araştırarak uygulamalı bir şekilde test etmektir. Çalışmada kullanılan araç olan Ddosphere, özelleştirilmiş bir DDoS saldırı simülasyon aracıdır. Saldırıların tasarlanması, uygulanması ve sonuçlarının analiz edilmesinde kullanılmıştır.

Ddosphere, kullanıcıların DDoS saldırı testlerini kolayca tasarlayabilmesini, uygulayabilmesini ve sonuçları analiz edebilmesini sağlayan güçlü bir platformdur. Kullanıcı dostu arayüzü ve gelişmiş özellikleri ile Ddosphere, siber güvenlik alanında DDoS saldırı testlerinin gerçekleştirilmesinde önemli avantajlar sunmaktadır. Bu platform, saldırıların gerçek zamanlı olarak izlenmesi, çeşitli metriklerle raporlanması ve farklı saldırı türlerinin karşılaştırılabilmesi gibi özellikler sunar.

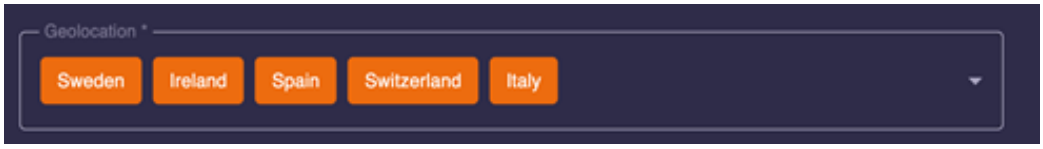
Bu çalışmada, aynı hedef URL'lere yapılan saldırılar incelenmiş ve iki farklı test gerçekleştirilmiştir. Bu testler, Ddosphere'in saldırı tiplerinden bağımsız olarak etkinliğini ve ağ performansına etkilerini ölçmeyi amaçlamıştır. Uygulanan yöntemler aşağıda detaylandırılmıştır:

3.1. Ddosphere ve Saldırı Tipleri *(Ddosphere and Attack Types)*

3.1.1. Saldırı Tipleri *(Attack Types)*

Ddosphere, geniş bir yelpazede yaklaşık 90 saldırı tipi sunar. Bu çalışmada, saldırı tiplerinden bağımsız olarak tek lokasyon ve çoklu lokasyon saldırıları gerçekleştirilmiştir (Şekil 1 ve Şekil 2).

Şekil 1. Tekli Lokasyon *(Single Location)*



Şekil 2. Çoklu Lokasyon *(Multiple Locations)*

3.1.2. Lokasyon Seçimi *(Location Selection)*

Çalışmada, çoklu lokasyon saldırıları için beş farklı coğrafi konum seçilmiştir. Bu seçim, gerçekçi bir DDoS botnet saldırısını simüle etmek için yapılmıştır. Farklı coğrafi konumlar, saldırıların dünya

çapında çeşitli noktalardan gerçekleştirilebilmesi ve ağ performansının bu farklılıklar karşısında nasıl değiştiğinin gözlemlenmesi amacıyla seçilmiştir.

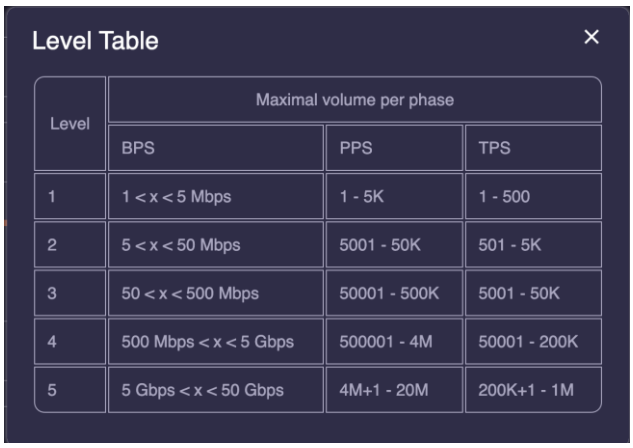
3.2. Saldırı Trafiği Modelleme *(Attack Traffic Modeling)*

3.2.1. Volumetrik Saldırılar *(Volumetric Attacks)*

Saldırılar, volumetrik saldırılar olarak planlanmış ve hedef sistemin bant genişliği ve kaynaklarını tüketmeyi amaçlamıştır. Bu tür saldırılar, ağ trafiğini büyük ölçüde artırarak hedef sistemin hizmet veremez hale gelmesini hedefler.

3.2.2. Saldırı Seviyeleri *(Attack Levels)*

Ddosphere'de saldırıların etkisi, farklı seviyelere göre değişiklik göstermektedir. Her seviyede, gönderilen trafik miktarı (BPS), paket sayısı (PPS) ve işlem sayısı (TPS) artış göstermektedir. Aşağıdaki tabloda, her seviye için belirlenen aralıklar verilmiştir (Şekil 3).


Level Table

Level	Maximal volume per phase		
	BPS	PPS	TPS
1	1 < x < 5 Mbps	1 - 5K	1 - 500
2	5 < x < 50 Mbps	5001 - 50K	501 - 5K
3	50 < x < 500 Mbps	50001 - 500K	5001 - 50K
4	500 Mbps < x < 5 Gbps	500001 - 4M	50001 - 200K
5	5 Gbps < x < 50 Gbps	4M+1 - 20M	200K+1 - 1M

Şekil 3. Saldırı seviyeleri *(Attack Levels)*

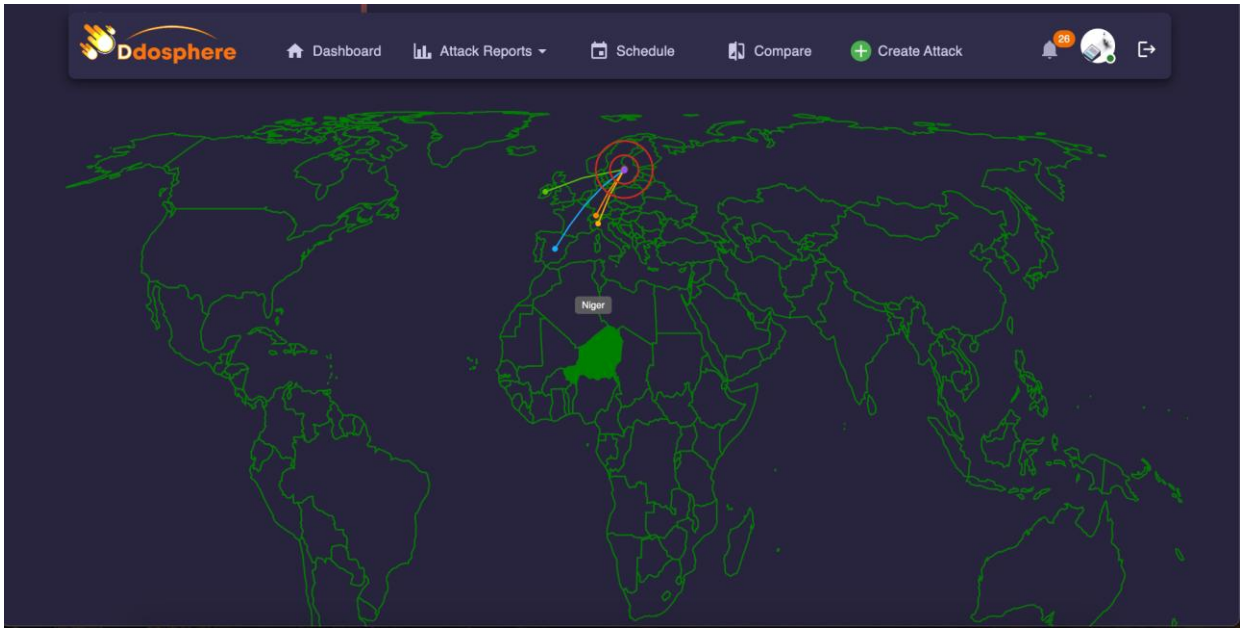
3.3. Test Altyapısı *(Test Infrastructure)*

3.3.1. Dağıtık Mimari *(Distributed Architecture)*

Kubernetes, Docker ve Amazon teknolojileri kullanılarak dağıtık bir mimari oluşturulmuş, farklı sunucular ve coğrafi konumlardan saldırılar gerçekleştirilmiştir. Bu teknoloji, saldırıların esnek bir şekilde yönetilmesini ve ölçeklenmesini sağlar. Kubernetes, konteynerleştirilmiş uygulamaların otomatik dağıtımı, ölçeklenmesi ve yönetimi için kullanılmıştır. Docker, uygulamaların konteynerleştirilmesi için kullanılmıştır. Amazon EC2 bulut sunucuları, farklı coğrafi konumlarda saldırı kaynaklarını simüle etmek için kullanılmıştır.

3.3.2. Canlı Saldırı İzleme *(Live Attack Monitoring)*

Ddosphere, saldırı sırasında anlık olarak gönderilen trafik miktarını ve sistemin sağlık durumunu izleyebilme özelliği sunar. Bu, saldırının etkilerinin gerçek zamanlı olarak değerlendirilmesini sağlar. Anlık izleme sayesinde, saldırı sırasında ne kadar trafik gönderildiği ve hedef sistemin bu trafik karşısındaki durumu sürekli olarak takip edilebilir (Şekil 4).



Şekil 4. Anlık İzleme Sistemi *(Real-Time Monitoring System)*

3.4. Testlerin Gerçekleştirilmesi *(Conducting the Tests)*

3.4.1. Tek Lokasyon Saldırısı *(Single Location Attack)*

Sadece bir sunucudan gelen saldırı trafiği kullanılmıştır. Bu test, tek bir kaynaktan gelen saldırıların sistem üzerindeki etkilerini değerlendirmek için yapılmıştır.

3.4.2. Çoklu Lokasyon Saldırısı *(Multiple Location Attack)*

Beş farklı coğrafi konumdan gelen saldırı trafiği kullanılmıştır. Bu test, dağıtık bir saldırı ortamında sistemin nasıl tepki verdiğini anlamak için yapılmıştır.

3.5. Performans Metrikleri *(Performance Metrics)*

3.5.1. Gecikme Süresi *(Latency)*

Saldırı öncesi ve sonrası ağ gecikme süreleri karşılaştırılmıştır. Gecikme süresi, ağın ne kadar hızlı yanıt verdiğini ve saldırı altında ne kadar yavaşladığını gösterir. Gecikme süresi, ICMP echo request/reply (ping) kullanılarak ölçülmüştür.

3.5.2. Bant Genişliği Kullanımı *(Bandwidth Usage)*

Saldırı sırasında kullanılan bant genişliği miktarı incelenmiştir. Bu, saldırının ne kadar yoğun olduğunu ve sistemin bant genişliğini ne kadar tükettiğini gösterir. Bant genişliği kullanımı, ağ trafiği izleme araçları (örneğin, iftop veya netflow) kullanılarak ölçülmüştür.

3.5.3. Servis Kesintisi *(Service Interruption)*

Saldırı nedeniyle meydana gelen olası servis kesintileri kaydedilmiştir. Bu, saldırının sistemde ne kadar süreyle hizmet kesintisine yol açtığını gösterir. Servis kesintileri, hedef sistemin yanıt vermemesi veya HTTP 503 (Service Unavailable) hataları döndürmesi durumunda kaydedilmiştir.

3.6. Gelişmiş Raporlama ve Karşılaştırma *(Advanced Reporting and Comparison)*

3.6.1. Saldırı Sonrası Raporlama *(Post-Attack Reporting)*

Saldırı sonrasında Ddosphere, gelişmiş raporlama özellikleri sunar. Bu raporlarda, saldırı sırasında gönderilen trafik miktarı, paket kaybı, gecikme süresi ve bant genişliği kullanımı gibi parametreler detaylı bir şekilde analiz edilir.

3.6.2. Rapor Karşılaştırma *(Report Comparison)*

Birden fazla DDoS saldırısının raporları karşılaştırılabilir, bu sayede zaman içindeki değişimler ve farklı saldırı tiplerinin etkileri değerlendirilebilir. Rapor karşılaştırmaları, sistemin farklı saldırı senaryolarına karşı ne kadar dayanıklı olduğunu gösterir.

3.6.3. Zamanlayıcı Kullanımı *(Use of Timer)*

Ddosphere, saldırıların belirli zamanlarda otomatik olarak başlatılabilmesi için zamanlayıcı kurma özelliği sunar. Bu özellik, saldırı testlerinin planlı bir şekilde gerçekleştirilmesini ve sistemin sürekli olarak test edilmesini sağlar.

3.7. Ddosphere ve Diğer Simülasyon Araçları Karşılaştırması *(Comparison of Ddosphere and Other Simulation Tools)*

Ddosphere, Dağıtık Hizmet Reddi (DDoS) saldırılarını simüle etmek için geliştirilmiş bir araçtır. Piyasada LOIC, HOIC, HULK gibi çeşitli DDoS simülasyon araçları bulunmaktadır. Ddosphere'i diğerlerinden ayıran temel farklar, avantajlar ve dezavantajlar aşağıda detaylandırılmıştır (Tablo 2).

3.7.1. Temel Farklar *(Key Differences)*

Mimari ve Ölçeklenebilirlik: Ddosphere, dağıtık ve ölçeklenebilir bir mimariye sahiptir. Bu, çok daha büyük ve karmaşık DDoS saldırılarını simüle etmesine olanak tanır. LOIC ve HOIC gibi araçlar genellikle tek bir makineden çalışır ve ölçeklenebilirlikleri sınırlıdır [4].

Saldırı Türleri ve Özelleştirme: Ddosphere, çeşitli DDoS saldırı türlerini (örneğin, TCP Flood, UDP Flood, HTTP Flood) destekler ve saldırı parametrelerinin detaylı bir şekilde özelleştirilmesine imkan verir. Diğer araçlar genellikle daha sınırlı saldırı türleri sunar ve özelleştirme seçenekleri daha azdır [6].

Gerçekçilik ve Simülasyon Doğruluğu: Ddosphere, gerçek dünya senaryolarına daha yakın simülasyonlar oluşturmayı hedefler. Ağ trafiği ve saldırı desenlerini daha gerçekçi bir şekilde taklit eder. LOIC ve HOIC gibi araçlar, basit ve temel saldırılar üretir, bu da gerçekçiliklerini azaltır [20].

Kullanım Kolaylığı ve Arayüz: Ddosphere, kullanıcı dostu bir arayüz ve kolay yapılandırma seçenekleri sunar. Diğer araçların arayüzleri daha karmaşık veya teknik bilgi gerektirebilir [10].

Tablo 2. Karşılaştırma tablosu *(Comparison Table)*

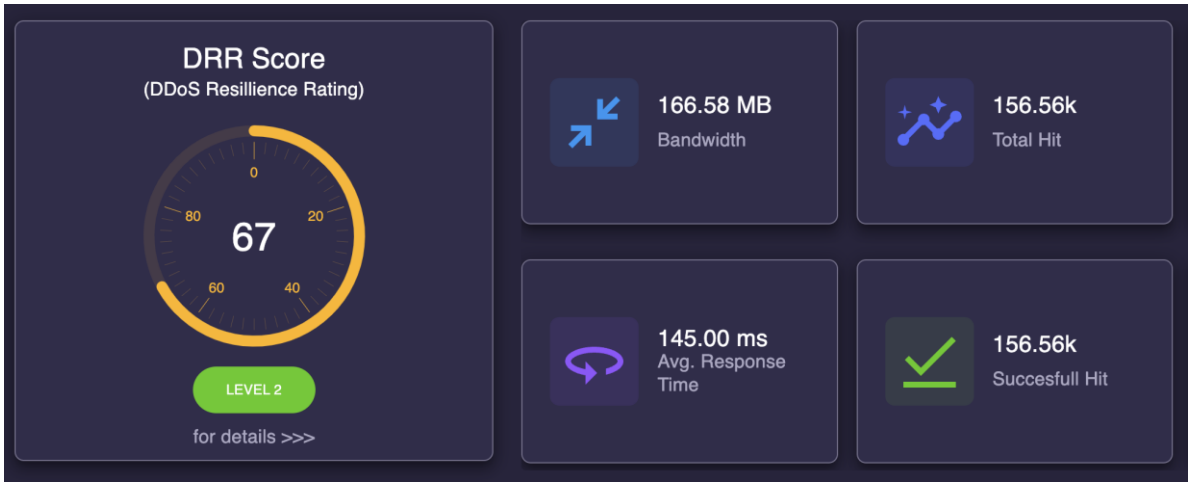
Özellik	Ddosphere	LOIC	HOIC	HULK
Mimari	Dağıtık, Ölçeklenebilir	Tek Makine	Tek Makine	Tek Makine
Saldırı Türleri	Geniş ve Özelleştirilebilir	Sınırlı	Sınırlı	Sınırlı
Ölçeklenebilirlik	Yüksek	Düşük	Düşük	Düşük
Gerçekçilik	Yüksek	Düşük	Düşük	Düşük
Kullanım Kolaylığı	Yüksek	Orta	Orta	Orta
Özelleştirme	Yüksek	Düşük	Düşük	Düşük

4. Bulgular *(Findings)*

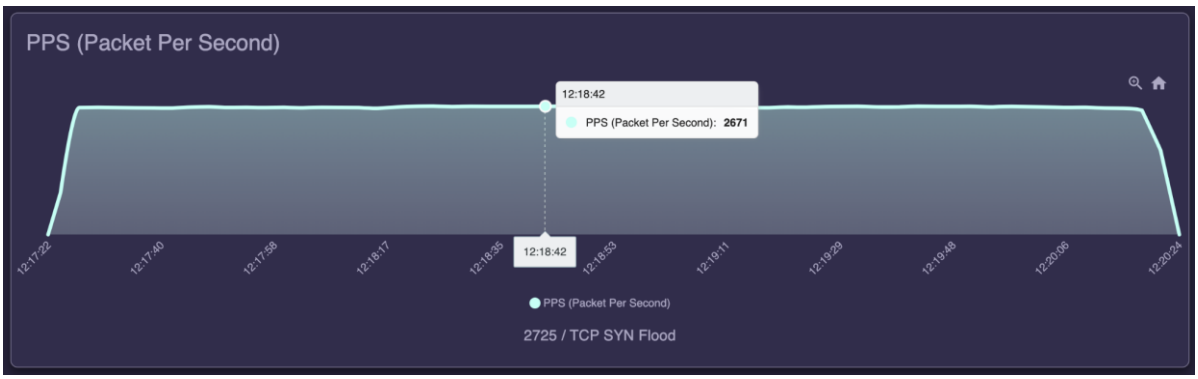
Bu bölümde, yapılan testlerin sonuçları incelenerek tek ve çoklu konumlu saldırıların ağ performansı üzerindeki etkileri karşılaştırmalı olarak sunulmaktadır.

4.1. Tek Lokasyon Saldırısı *(Single Location Attack)*

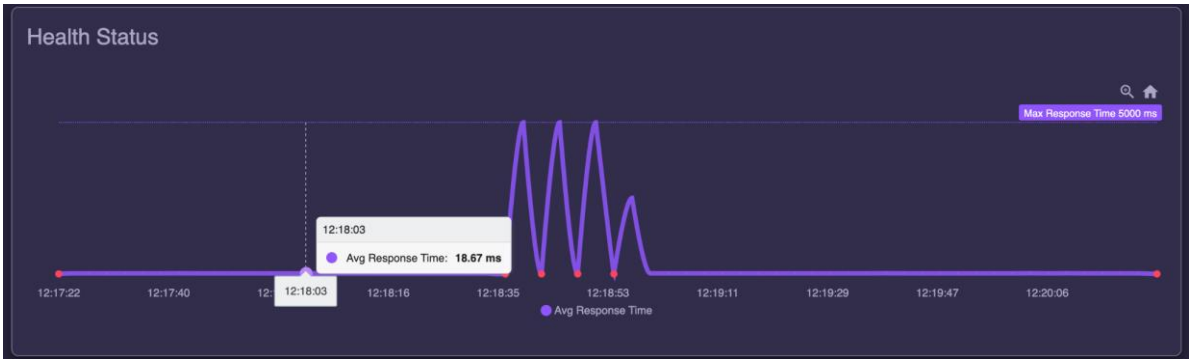
Gecikme Süresi. Ortalama gecikme süresi 18 ms'den 145 ms'ye yükselmiştir (Şekil 5). Bant Genişliği Kullanımı. Saldırı trafiği 166.58 MB olarak ölçülmüştür (Şekil 6). Servis Kesintisi. Kısa süreli (yaklaşık 24 saniyelik) servis kesintileri raporlanmıştır (Şekil 7).



Şekil 5. Tek lokasyon saldırısı sırasındaki gecikme süresi değişimi *(Latency variation during the single location attack)*



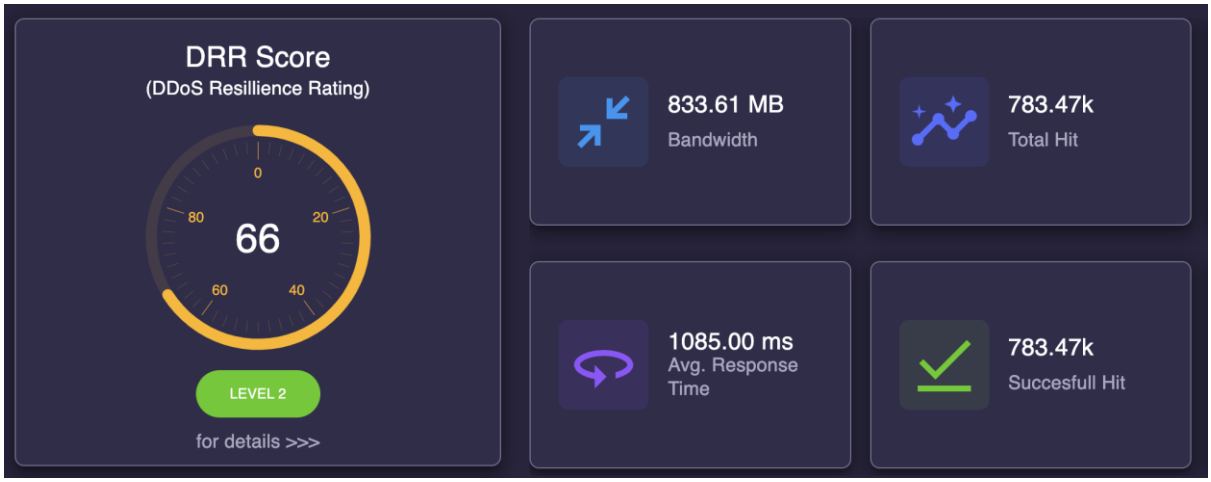
Şekil 6. Tek lokasyon saldırısı sırasındaki bant genişliği kullanımı *(Bandwidth usage during the single location attack)*



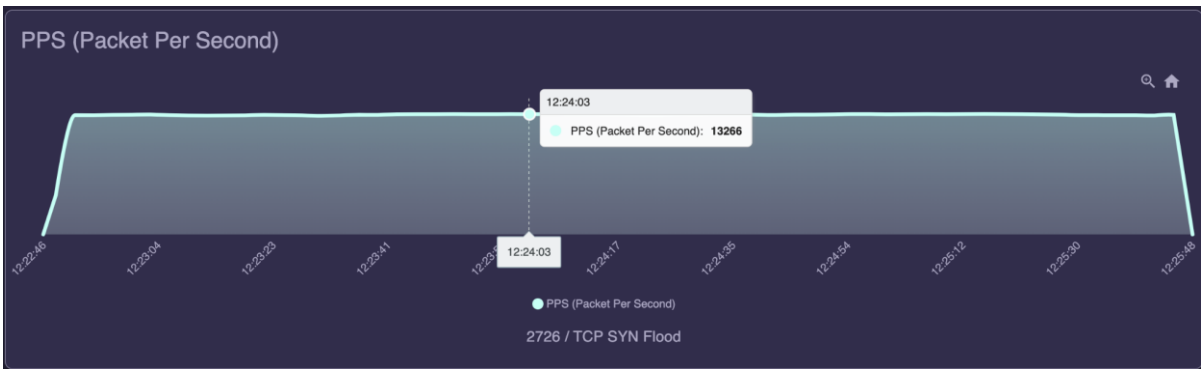
Şekil 7. Tek lokasyon saldırısı sırasında raporlanan servis kesintileri *(Service interruptions reported during the single location attack)*

4.2. Çoklu Lokasyon Saldırısı *(Multiple Location Attack)*

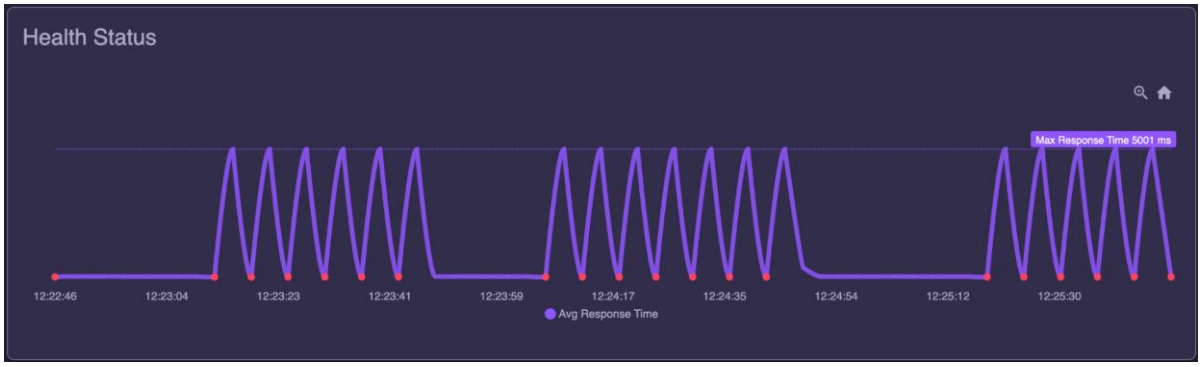
Gecikme Süresi. Ortalama gecikme süresi 18 ms'den 1045 ms'ye çıkmıştır (Şekil 8). Bant Genişliği Kullanımı. Saldırı trafiği 833.61 MB olarak ölçülmüştür (Şekil 9). Servis Kesintisi. Uzun süreli (yaklaşık 108 saniyelik) servis kesintileri yaşanmıştır (Şekil 10).



Şekil 8. Çoklu lokasyon saldırısı sırasındaki gecikme süresi değişimi *(Latency variation during the multiple location attack)*



Şekil 9. Çoklu lokasyon saldırısı sırasındaki bant genişliği kullanımı *(Bandwidth usage during the multiple location attack)*



Şekil 10. Çoklu Lokasyon Saldırısı Sırasında Raporlanan Servis Kesintileri *(Service interruptions reported during the multiple location attack)*

4.3. Genel Değerlendirme *(Overall Evaluation)*

4.3.1. Tek lokasyon vs. çoklu lokasyon *(Single Location vs. Multiple Location)*

Tek lokasyondan gelen saldırılar, çoklu lokasyon saldırılarına göre daha az zararlı olmuştur. Çoklu lokasyondan gerçekleştirilen saldırılar, ağ performansını ciddi şekilde düşürmüş ve daha fazla hizmet kesintisine yol açmıştır.

4.3.2. Ddosphere'in etkinliği *(Effectiveness of Ddosphere)*

Ddosphere, geniş saldırı yelpazesi, dağıtık saldırı kapasitesi ve gelişmiş raporlama özellikleri ile ağ performansını değerlendirmede etkili bir araç olarak görülmüştür.

Bu çalışma, Ddosphere'in sunduğu geniş saldırı çeşitliliği, dağıtık saldırı kapasitesi ve gelişmiş raporlama özellikleri ile tek lokasyondan yapılan saldırılara kıyasla, çoklu lokasyonlardan yapılan DDoS saldırılarının ağ performansına çok daha ciddi etkiler yarattığını göstermiştir. Çalışma sonucunda, çoklu lokasyon saldırılarının ağ performansını daha fazla düşürdüğü ve daha uzun süreli hizmet kesintilerine yol açtığı belirlenmiştir. Bu bulgular, ağ performansını korumak ve hizmet kesintilerini en aza indirmek için daha güçlü ve dağıtık saldırılara karşı daha dirençli savunma mekanizmalarının geliştirilmesi gerektiğini ortaya koymaktadır.

5. Sonuç *(Conclusion)*

Sonuç olarak, bu çalışma, çoklu lokasyonlardan gelen DDoS saldırılarının ağ performansı üzerindeki yıkıcı etkilerini net bir şekilde ortaya koymuştur. Tek lokasyondan gelen saldırılara kıyasla, çoklu lokasyonlardan gerçekleştirilen saldırılar, ağ performansını daha fazla düşürmüş ve daha uzun süreli hizmet kesintilerine yol açmıştır. Bu bulgular, ağ güvenliğini sağlamak ve hizmet kesintilerini minimize etmek için daha güçlü ve dirençli savunma mekanizmalarının geliştirilmesi gerektiğini göstermektedir.

Ddosphere aracı, sunduğu geniş saldırı yelpazesi ve dağıtık saldırı kapasitesi ile bu tür senaryo ve simülasyonlarda etkili bir araç olduğunu kanıtlamıştır. Bu çalışma, ağ yöneticileri ve siber güvenlik uzmanları için değerli içgörüler sunulmakta olup, gelecekteki siber tehditlere karşı hazırlıklı olmak adına savunma stratejilerinin gözden geçirilmesi ve güçlendirilmesi gerektiğini vurgulamaktadır. Siber güvenlik alanındaki bu tür araçların önemi, sadece mevcut tehditlere karşı değil, aynı zamanda ağ performansını optimize etmek ve olası hizmet kesintilerini en aza indirmek için yapılacak iyileştirmeler açısından da kritik bir rol oynamaktadır.

Bu çalışma, ağların DDoS saldırılarına karşı korunması için daha geniş çaplı araştırmaların ve geliştirmelerin gerekliliğini de ortaya koymaktadır. Gelecekteki araştırmalar, bu tür saldırılara karşı daha sofistike ve entegre savunma mekanizmalarının geliştirilmesine katkı sağlayabilir.

Teşekkür ve Finansman ***(Acknowledgments and Funding)***

Bu çalışmanın özet hali, 21. UBAK Uluslararası Bilimsel Araştırmalar Kongresi'nde (12-13 Ekim 2024) sunulmuştur.

Kaynaklar ***(References)***

[1] A. Hussain, J. Heidemann, C. Papadopoulos, “Distinguishing between single and multi-source attacks using signal processing”, Computer Networks 46:4 (2004) 479–503. Doi:10.1016/j.comnet.2004.02.003.

[2] A. Chadd, “DDoS attacks: past, present and future”, Network Security 2018:7 (2018) 13–15. Doi:10.1016/S1353-4858(18)30069-2.

[3] D. Dittrich, “The DoS Project's 'trinoo' distributed denial of service attack tool”, University of Washington (1999). Available: https://staff.washington.edu/dittrich/misc/trinoo.analysis.txt.

[4] V. Paxson, "An analysis of using reflectors for distributed denial-of-service attacks." ACM SIGCOMM Computer Communication Review, 31(3), 38–47 (2001).

[5] D. Goodin, "Mafiaboy and the Yahoo Attack of 2000." Ars Technica (2010).

[6] D. Moore, C. Shannon, G. M. Voelker, S. Savage, “Internet quarantine: requirements for containing self-propagating code”, IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No.03CH37428), San Francisco, CA, USA 3 (2003) 1901–1910. Doi:10.1109/INFCOM.2003.1209212.

[7] M. Prince, “The DDoS That Almost Broke the Internet”, Cloudflare Blog (2013). Available: https://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet/.

[8] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, et al., “Understanding the Mirai Botnet”, Proceedings of the 26th USENIX Security Symposium (2017) 1093–1110. Available: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis.

[9] S. Hilton, “The GitHub 1.35Tbps DDoS Attack Breakdown”, KrebsOnSecurity (2018).

[10] AWS Security Team, “Mitigating the Largest DDoS Attack on Record”, AWS Shield Threat Landscape Report – Q1 2020 (2020).

[10] O. Yoachimik, “Cloudflare mitigates 26 million request per second DDoS attack”, Cloudflare Blog (2022). Available: https://blog.cloudflare.com/26m-rps-ddos-attack/.

[12] J. Anderson and B. Smith, “AI-Driven Botnets and the Future of DDoS Attacks”, ACM Transactions on Cybersecurity (2023).

[13] S. Nakamoto, “DDoS Attacks on Web3 Infrastructure: Challenges and Countermeasures”, IEEE Transactions on Network Security (2024).

[14] C. Douligeris, & A. Mitrokotsa, “DDoS attacks and defense mechanisms: classification and state-of-the-art”, Computer Networks, 44(5), 643–666 (2004). https://doi.org/10.1016/j.comnet.2003.10.003

[15] H. Harshita, “Detection and Prevention of ICMP Flood DDoS Attack”, International Journal of New Technology and Research 3:3 (2017) 63–69. Available: https://www.neliti.com/publications/263333/detection-and-prevention-of-icmp-flood-ddos-attack

[16] M. Bogdanoski, T. Shuminoski, A. Risteski, “Analysis of the SYN flood DoS attack”, International Journal of Computer Network and Information Security 5:8 (2013) 1–11. Doi:10.5815/ijcnis.2013.08.01.

[17] E. Kumara, “Lesson 2: DoS Attacks, Spoofing, Smurf Attacks, and Phishing”, Tugas Jaringan Komputer, Universitas Sriwijaya, Fakultas Ilmu Komputer, Sistem Komputer SK5C, (2018), 2 s. Erişim: https://edocs.ilkom.unsri.ac.id/1880/1/Tugas6_09011281520098.pdf

[18] A. R. Shaaban, E. Abdelwaness, M. Hussein, “TCP and HTTP Flood DDoS Attack Analysis and Detection for Space Ground Network”, 2019 IEEE International Conference on Vehicular Electronics and Safety (ICVES), Cairo, Egypt, 2019, pp. 1–6. Doi:10.1109/ICVES.2019.8906361.

[19] S. Sabri, N. Ismail, A. Hazzim, “Slowloris DoS Attack Based Simulation”, IOP Conference Series: Materials Science and Engineering, vol. 1062, no. 1, 2021, p. 012029. Doi:10.1088/1757-899X/1062/1/012029.

[20] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, ... Y. Zhou, “Understanding the Mirai Botnet”, 26th USENIX Security Symposium (USENIX Security 17) (2017) 1093–1110. Available: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis.

[21] G. Kambourakis, T. Moschos, D. Geneiatakis, S. Gritzalis, “Detecting DNS Amplification Attacks”, in Critical Information Infrastructures Security, J. Lopez & B. M. Hämmerli (eds.), Lecture Notes in Computer Science, vol. 5141, Springer, Berlin, Heidelberg, 2008, pp. 185–196. doi:10.1007/978-3-540-89173-4_16

[22] L. Rudman, B. Irwin, “Characterization and Analysis of NTP Amplification Based DDoS Attacks”, 2015 Information Security for South Africa (ISSA) (2015) 1–5. Doi:10.1109/ISSA.2015.7335052.

[23] T. Rozekrans, M. Mekking, J. de Koning, “Defending against DNS Reflection Amplification Attacks”, University of Amsterdam, System and Network Engineering Research Project 1 (RP1) (2013) 1–24. Available: https://www.nlnetlabs.nl/downloads/publications/report-rrl-dekoning-rozekrans.pdf.

[24] L. Rudman, “Analysis of NTP Based Amplification DDoS Attacks”, Technical Report, 2014, pp. 1–18. Available: https://digifors.cs.up.ac.za/issa/2015/Proceedings/Full/71_Paper.pdf

[25] C. Sheth, R. Thakker, “Performance Evaluation and Comparison of Network Firewalls under DDoS Attack”, International Journal of Computer Network and Information Security, vol. 5, no. 12, pp. 60–67, 2013. doi:10.5815/ijcnis.2013.12.08.

[26] M. Sachdeva, K. Kumar, G. Singh, K. Singh, “Performance Analysis of Web Service under DDoS Attacks”, in 2009 IEEE International Advance Computing Conference, Patiala, India, Mar. 2009, pp. 1002–1007. doi:10.1109/IADCC.2009.4809190.