T.C.
GEBZE TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

SDN TABANLI DAĞITIK SALDIRI TESPİT VE ÖNLEME SİSTEMİ

KAAN ÖZDİNÇER
YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

GEBZE
2020

T.C.
GEBZE TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

SDN TABANLI DAĞITIK SALDIRI TESPİT VE ÖNLEME SİSTEMİ

KAAN ÖZDİNÇER

YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

DANIŞMANI
PROF. DR. HACI ALİ MANTAR

GEBZE
2020

T.R.

GEBZE TECHNICAL UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

SDN BASED DISTRIBUTED INSTRUSION DETECTION AND PREVENTION SYSTEM

KAAN ÖZDİNÇER

A THESIS SUBMITTED FOR THE DEGREE OF

MASTER OF SCIENCE

DEPARTMENT OF COMPUTER ENGINEERING

THESIS SUPERVISOR

PROF. DR. HACI ALİ MANTAR

GEBZE

2020

GEBZE TEKNİK ÜNİVERSİTESİ	YÜKSEK LİSANS JÜRİ ONAY FORMU

GTÜ Fen Bilimleri Enstitüsü Yönetim Kurulu'nun 03/07/2019 tarih ve 2019/30 sayılı kararıyla oluşturulan jüri tarafından 21/11/2019 tarihinde tez savunma sınavı yapılan Kaan Özdinçer'ın tez çalışması Bilgisayar Mühendisliği Anabilim Dalında YÜKSEK LİSANS tezi olarak kabul edilmiştir.

JÜRİ

ÜYE (TEZ DANIŞMANI)	: Prof. Dr. Hacı Ali Mantar
ÜYE	: Doç. Dr. Hasari Çelebi
ÜYE	: Doç. Dr. Muhammed Ali Aydın

ONAY

Gebze Teknik Üniversitesi Fen Bilimleri Enstitüsü Yönetim Kurulu'nun

...../...../..... tarih ve ...../..... sayılı kararı.

ÖZET

DNS kuvvetlendirme saldırısı bir tür yansıtma tabanlı, Dağıtık Hizmet Engelleme (Distributed Denial of Service, DDoS) saldırısıdır. Ağdaki kurbanların güvenilirliği ve dayanıklılığı açısından çok tehlikelidir. Bu tür saldırıları önlemek veya etkilerini azaltmak için hem geleneksel ağlarda, hem de Yazılım Tanımlı Ağlarda (Software Defined Networks, SDN) önemli miktarda çalışma yapılmaktadır. Bu çalışma, DNS tabanlı kuvvetlendirme saldırılarının, SDN tabanlı ağlardaki etkilerini tespit etmek ve azaltmak amacıyla yapılmıştır. Bu sistem, önleme sistemini başlatmak ve kurbanın yaşamını sürdürebilmesi için, Kuvvetlendirme Faktörü (Amplification Factor, AF) ve TTL (Time to Live), Hop Sayısı Değişimi (Hop Count Variation, HCV) hesaplayarak saldırıyı izlemeyi amaçlamaktadır. Bunu yaparken, metrikleri bir zaman serisi veri tabanına (Time Series Database, TSDB) kaydetmekte alarmlar üretmekte ve saldırının etkilerini azaltmaktadır. Deneysel sonuçlar, bu sistemin SDN tabanlı ağlarda kullanılabileceği ve reaktif bir şekilde saldırıyı önleyebileceğini göstermektedir. Ayrıca sadece DNS kuvvetlendirme/yansıtma saldırıları için değil UDP (User Datagram Protocol) tabanlı tüm kuvvetlendirme saldırıları için de kullanılabileceği görülmüştür.

Anahtar Kelimeler: DNS Amplification, SDN, DDoS , Amplification Factor, TTL, AF, HCV.

SUMMARY

DNS amplification is a type of reflection-based DDoS attacks, and they are very hazardous for the reliability of victims within the network. To prevent or mitigate such attacks, a significant amount of work is being done both on conventional networks and on SDN-based networks. This study aimed to detect and reduce the effects of DNS amplification attacks in SDN-based with the developed system. This system aims to monitor the variations in the amplification factor and TTL header to initiate mitigation and sustain the victim's life. It also ensures that legitimate packets are not suspected in the process. In doing so, it is aimed to generate alarms and mitigation by using the central management feature of SDN, by writing the metrics into a time series database immediately. Experimental results show that this system can be used SDN-based networks and prevent an attack in reactively. It has also been observed that it can be used not only for DNS amplification attacks but also for other UDP-based amplification/reflection attacks.

Key Words: DNS Amplification, SDN, DDoS , Amplification Factor, TTL, AF, HCV.

TEŞEKKÜR

Başta, yüksek lisans eğitimimin tamamında ve bu çalışmada verdiği destek, öneriler için, danışmanım Prof. Dr. Hacı Ali Mantar'a,

Birçok konuda verdiği ömürlük destek, vizyon ve öneriler için, lisans eğitimimden Hocam ve şimdiki can arkadaşım Dr. Necdet Yücel'e,

Bu eğitim ve çalışmam için gerekli olan zamanı yaratmamdaki yardımları için, iş arkadaşlarım İşbaran Akçayır ve Okan Özdemir'e,

Verdikleri koşulsuz destek ve sabır için Ailem, Rabia Özdinçer, Erdoğan Özdinçer ve Ozan Özdinçer'e, sonsuz teşekkür ederim.

İÇİNDEKİLER

SİMGELER ve KISALTMALAR DİZİNİ

Simgeler ve Kısaltmalar		**Açıklamalar**
SDN	:	Software Defined Networking
YTA	:	Yazılım Tanımlı Ağlar
DDoS	:	Distributed Denial of Service
DRDoS	:	Distributed Reflective Denial of Service
DNS	:	Domain Name System
NTP	:	Network Time Protocol
IP	:	Internet Protocol
IoT	:	Internet of Things
VPN	:	Virtual Private Network
SSL	:	Secure Sockets Layer
API	:	Application Programming Interface
Cots	:	Commercial off-the-shelf
TTL	:	Time to Live
HC	:	Hop Count
HCV	:	Hop Count Variation
AF	:	Amplification Factor
ML	:	Machine Learning
DPI	:	Deep packet inspection
Pcap	:	Packet Capture
ONF	:	Open Networking Foundation
TSDB	:	Time Series Database

ŞEKİLLER DİZİNİ

TABLOLAR DİZİNİ

1. GİRİŞ

SDN ve güvenlik hakkında konuşulduğunda, iki ana konu akla gelmektedir. Birincisi, SDN altyapısının güvenliği ve SDN tabanlı ağ tarafından kullanılan protokolün (Örn: Openflow) güvenliği. İkicisi ise, SDN tabanlı güvenlik uygulamalarıdır. Bu çalışmada, ikinci konunun bir alt dalı incelenecektir.

Scott-Hayward'ın çalışmasında [1] belirtildiği gibi, SDN tabanlı güvenlik uygulamaları üzerinde kayda değer miktarda çalışma yapıldığı görülmüştür. Ayrıca birçok güvenlik açığı üstüne de çalışmalar yapılmıştır. Yetkisiz erişime, denetleyici olmadan gelen misafire karşı korumaya, dağıtık denetim modeline ve buna karşı yasaklı erişimi anlayan akıllı sistemlere karşı çözümler üretilmiştir. Ağdaki kötü amaçlı uygulamalara yönelik çözümler şunlardır: Talebe göre kaynak belirleme, uygulama davranışlarına bakarak tespit ve engellenmesi, olası ağ sorunlarını gidermek için yeni yollar belirleme vb. Genellikle ağ saldırılarına karşı atılan adımlar ise şunlardır: Ağ desenlerine göre saldırıyı anlamak ve gerekli ayarları yapmak, denetleyiciyi ölçeklemek, kaynak adresi doğrulamak, gerçek zamanlı ağ izleme, yanlış yapılandırma ve çakışmaları anlamak vb. Denetleyici ve kanalları seviyesindeki güvenlik için: Veri toplama, trafik analizi ve kuralların güncellenmesi, çevik ağ erişim denetimi, altyapı güvenliği sorunları, IoT gibi ağlarda geçici elemanların güvenliği için ağ izleme gibi yöntemler kullanılmaktadır.

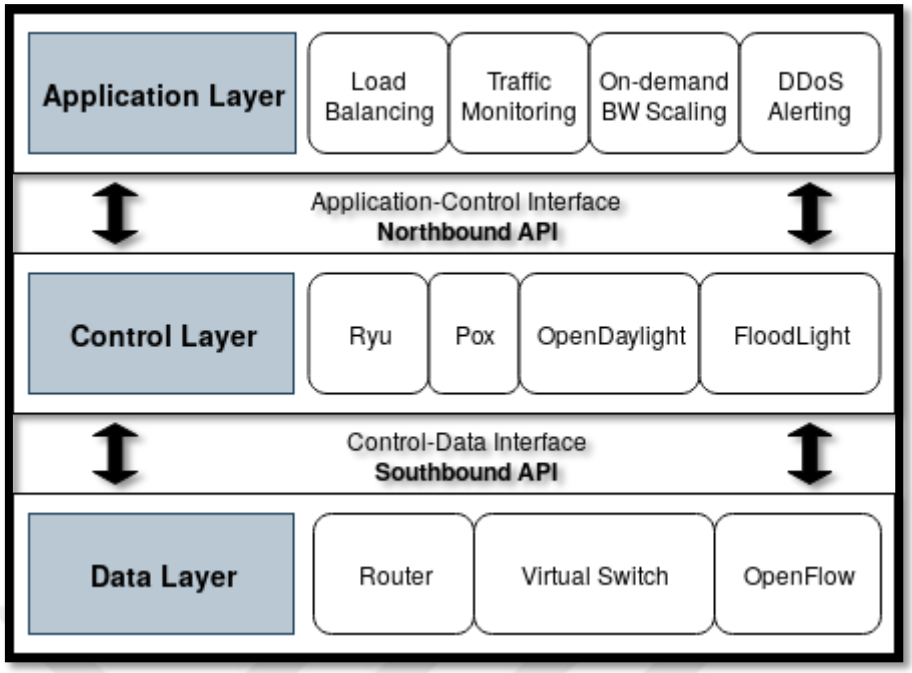
Bu çalışmada ise, iligi ağ bilgileri toplanacak ve bir DRDoS (Distributed Reflection Denial of Service) saldırısı türü olan DNS kuvvetlendirme saldırılarını önlemek için azaltma/engelleme aşaması gerçeklenecektir. Bu gerçekleme yapılırken, gerçek saldırıların olduğu bir veri seti ile çalışma yapılacaktır. Sırasıyla konuyla ilgili temel bilgiler verilecek, konuyla ilgili yapılmış birçok çalışma incelenecek, sorunun giderilmesi için bir öneri getirilecek ve gerçeklenecek, deney sonuçları değerlendirilecek ve son olarak sonuçlar değerlendirilip, bazı öneriler ortaya konulacaktır.

2. TEMEL BİLGİLER

Bu bölümde, temel bilgiler ayrıntılı bir şekilde anlatılacaktır. Yazılım Tanımlı Ağlar ve güvenlikle olan ilişkisi, SDN güvenlik vektörleri, DNS ve DNS Kuvvetlendirmeli DDoS saldırısına genel bir bakış yapılacaktır. Kavramlar ayrıntılı bir şekilde anlatılırken tablolar ve şekiller ile desteklenecektir.

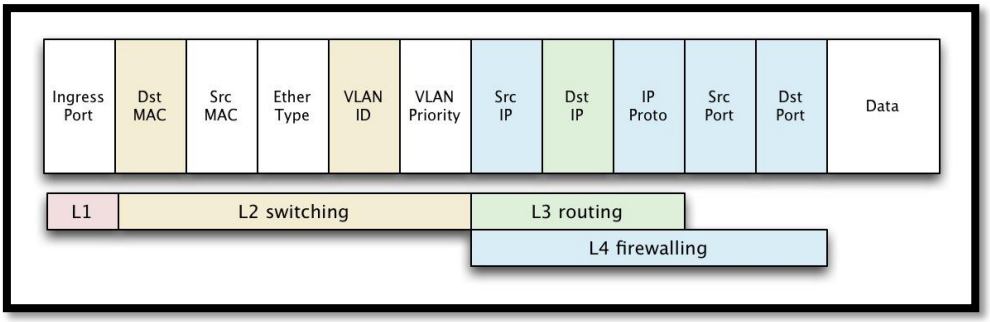
2.1. SDN ve Güvenlik

Yazılım Tanımlı Ağlar (ONF, 2012), bilgisayar ağlarını kolayca yönetmenin ve ağ araştırmalarının hızını arttırmanın yeni bir yoludur. Proje ilk olarak Sandford Üniversitesi'nin bir projesi olarak başladı ve OpenFlow protokolü, bu araştırmanın ilk ürünü olarak ortaya çıkmıştır. Aslında bir metodolojidir ve Şekil 2.1'de temel mimarisi gösterilmiştir. Ağ düzleminin programlanabilmesi için, ağ denetim düzlemi ve yönlendirme düzleminin birbirinden ayrılması amaçlanmaktadır. Böylece günümüzdeki uygulamaların, yüksek bant genişliğine sahip ve dinamik doğasına uygun şekilde, uzaktan yönetilebilir, ölçeklenebilir bilgisayar ağları gerçeklememizi sağlar. Doğrudan programlanabilir, çevik, merkezi yönetimi olan, programlayarak yapılandırılan ve açık standartlar tabanlı, böylece firma bağımlı olmayan ağlar gerçeklenebilir. Kritik güvenlik yamaları geldiğinde, bunları her cihazda elle yapılandırmak zor olabilir ve potansiyel olarak yanlış yapılandırmalara yol açabilir. SDN denetleyicisi ile birlikte, her cihaz fiziksel cihazlara erişmeye gerek kalmadan güncellenebilir. Bu, tüm güncellemelerin ağ boyunca doğru ve hızlı bir şekilde yayılabileceği anlamına gelmektedir. SDN üzerindeki güvenlik sorunlarından biri ise, saldırganların tüm ağ güvenliğinizin denetimini ele geçirmek için ağınızdaki tek bir düğüme (SDN denetleyicisi) erişmesi gerektiğidir. Bu nedenle güvenli bir SDN ağ sağlayıcısı seçmek ve SDN denetleyicisini dış tehditlerden koruyan güvenlik öğeleri kullanmak önemlidir. Yazılım tanımlı ağ, çok çeşitli ağ cihazlarını tek bir uygun platformda soyutlayabilir. Bu, bağlantıların korunmasını, kritik güncellemelerin yapılmasını ve önemli güvenlik sorunlarının karantinaya alınmasını basit ve etkili hale getirir. SDN aynı zamanda temas noktalarını azaltır, tekrarlanan görevleri yapmayı da kolaylaştırmaktadır.



Şekil 2.1: 3 Katmanlı SDN Mimarisi.

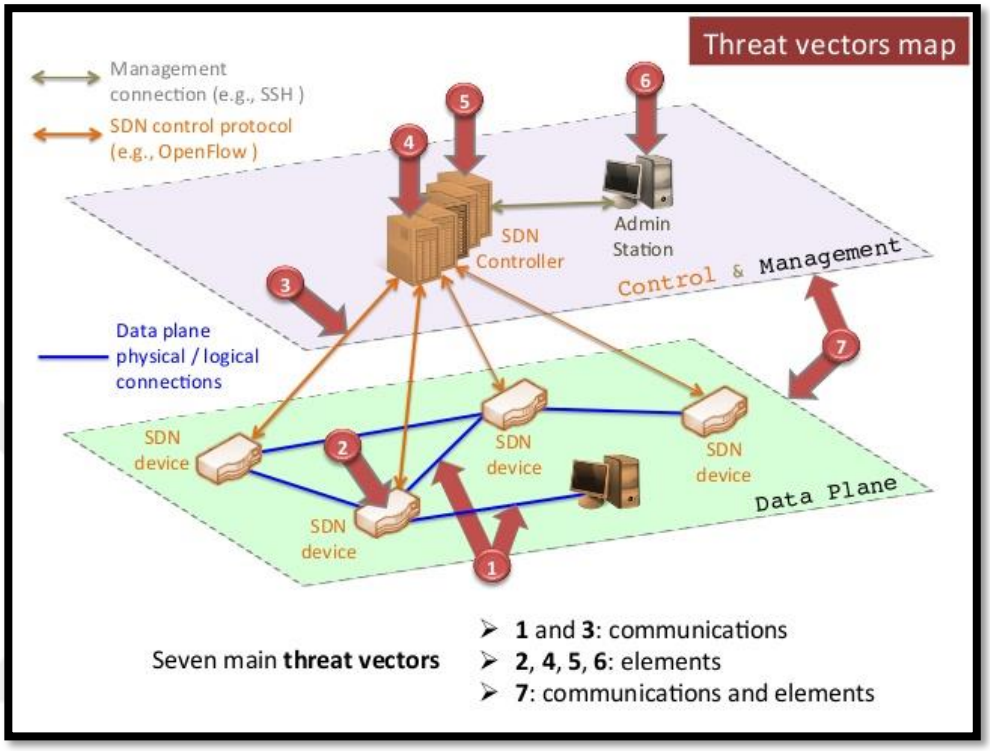
Bu altyapıda, son kullanıcılar ve bağımsız uygulamalar için bir uygulama katmanı bulunmaktadır. Bu katman içinde, northbound API adı da verilen ara yüzler bulunmaktadır. Denetim katmanında ise, OpenFlow üzerinde altyapısal değişiklik yapılmasına olanak tanır. Altyapı katmanında ise, temel ağ fonksiyonları olan yönlendirme işlemleri yapılır. Ayrıca bu model için anahtar özellikler bulunmaktadır. Bunları en başında mantıksal ve merkezileştirilmiş akıl bulunmaktadır. Şekil 2.2'de başlıkları verilen, OpenFlow protokolüyle haberleşen ve merkezi bir yerden yönetilen bir ağ hayal edilmelidir. Programlanabilirlik ve soyutlama ise diğer önemli özelliklerdir. Programlama yaklaşımıyla sürekli kendini yenileyebilen, değiştirebilen bir ağ ve protokol sayesinde soyut olarak görülebilen bir ağ altyapısı elde edilmektedir. OpenFlow ağ ekibine son derece ayrıntılı bir denetim sağlayarak ağın uygulama, kullanıcı ve oturum düzeylerindeki gerçek zamanlı değişikliklere yanıt vermesini sağlar. OpenFlow, ağ ekibinin kullanım modelleri, uygulama ihtiyaçları, hizmet düzeyi sözleşmeleri ve bulut kaynakları gibi parametrelere dayalı olarak, ağ aygıtları üzerinden trafiğin nasıl akması gerektiğini tanımlamasına olanak tanır.



Şekil 2.2: Openflow paket başlığı.

Böyle bir yaklaşıma olan ihtiyacın nedenleri arasında, sıklıkla değişen trafik örüntüleri vardır. Her sürümde, her yapılandırmada şekil değiştiren trafik akışına hızlıca uyum sağlamak gereklidir. Bunun dışında bulut bilişimdeki yükseliş, "Büyük Veri" kullanımındaki artış, karmaşıklaşan ağların yönetilemez duruma gelmesi, birbiriyle uyumsuz yaklaşımların oluşturduğu yapılandırmalar, ölçeklendirme sorunun giderek artması, donanım sağlayıcılara olan bağımlılıklar gibi sorunlar geleneksel ağlardan SDN'e geçiş için kabul edilebilir nedenlerdir. SDN bu sorunlara, çoklu donanım sağlayıcı desteğini merkezileştirme, otomasyondan doğan karmaşıklığı azaltma, yeniliğe uyumluluk, artırılmış ağ güvenliği ve sürdürülebilirliği, ağın her yerine kolay erişim ve daha iyi kullanıcı deneyimi gibi cevaplar getirmiştir. Günümüzdeki güvenlik çözümleri, güvenlik duvarları, saldırı tanıma ve engelleme sistemleri, SSL ve VPN çözümleri, merkezi ağ yönetim araçları, 802.1X port tabanlı kimlik doğrulama ve erişim denetimleri, IPsec tabanlı uçtan uca şifreli IP paketlerinden oluşan oturumlar, TLS tabanlı uygulama katmanı iletişimleri, RADIUS gibi merkezi kimlik doğrulama ve kimlik kanıtlama sistemlerini içermektedir. SDN mimarisi yukarıda anlatılan güvenlik çözümlerine, geleneksel yönlendirme sınırlamalarına karşı flow tabanlı güvenlik işleyişi, mantıksal ve merkezi gözlemleme ile ağa yukarıdan ve kapsamlı bir yönetim, her bir ağ elemanı için merkezi ve ayrıntılı politika belirleme, çeşitli risk grupları için güvenlik duvarı gibi çözümler ile gelmektedir. SDN ve güvenlik denilince akla iki başlık gelmektedir. Birincisi SDN'in ve kullanılan protokolün güvenlik yapısı. İkincisi ise, SDN tabanlı güvenlik uygulamalarıdır. Bu çalışmanın kendisi, ikinci başlığın konularından biridir. Bu nedenle birinci başlıktan konulara değinilmeyecektir.

SDN için yaygın olarak yanlış tanımlamalar yapılmaktadır. SDN, bir protokol, bir protokol ailesi, bir teknoloji, OpenFlow'un kendisi değildir. SDN, ONF liderliğinde tanımlanmış ölçeklenebilir, kolay yönetilebilir, denetim düzlemini yönlendirme düzleminden ayıran merkezi ve programlanabilir bir ağ yaklaşımı, bir konsept, bir metodolojidir.



Şekil 2.3: SDN Tehdit Vektörü Haritası.

Şu [2] çalışmada, SDN tabanlı güvenlik uygulamaları hakkında oldukça fazla bilgi bulunmaktadır. Ayrıca farklı güvenlik zafiyetleri üzerine çalışmalardan bahsedilmiştir. İzinsiz erişimlere karşı, denetleyiciyi saldırganlardan koruma, dağıtık denetim modeli, yasaklı erişimleri anlayan ve durum alan akıllı sistemler gibi çözümler görülmüştür. Ağda bulunan zararlı ve kötü niyetli uygulamaları engelleme, otomatik kaynak ihtiyacı karşılama, uygulamaların davranışlarına bakarak tespit ve engelleme, olası ağ sorunlarına otomatik yeni yollar tanımlama gibi çözümler görülmüştür. DoS saldırılarına karşı, ağ örüntülerinden saldırıyı anlayıp gerekli ağ ayarlarını yapma, denetleyiciyi ölçekleme, kaynak adres doğrulaması gibi çözümler üretildiği görülmüştür. Yanlış yapılandırmalara karşı, hızlı geri alma, ağın gerçek zamanlı izlenmesi, politika çakışmalarını belirleme gibi çözümlerin olduğu görülmüştür.

Sistem seviyesi SDN sorunlarına karşı, SDN hata ayıklayıcı, denetleyici iletişimini yapan denetim katmanın güvenliği gibi çözümler üretildiği görülmüştür. Genel bir bakış yapıldığında ise, trafik analizi ve kuralların güncellenmesi, DoS/DDoS koruması, Middlebox ve mimarinin kendi güvenlik sorunları, ölçekleme ve isteğe göre şekillenme gibi konuların çalışıldığı görülmüştür. Şuradaki [3] çalışmaya göre, Şekil 2.3'te ana tehdit vektörleri haritası gösterilmiş ve Tablo 2.1'de örnekleri açıklanmıştır.

Tablo 2.1: SDN'e özgü tehtidler ve sonuçları.

Tehdit Vektörü	**SDN'e özgü mü?**	**SDN'deki sonuçlar**
1	Hayır	DDoS saldırıları için açık kapı.
2	Hayır	Saldırı enflasyonu.
3	Evet	Merkezi denetleyicinin istismarı.
4	Evet	Saldırı altındaki denetleyicinin tüm ağı tehdidi.
5	Evet	Kötü niyetli denetleyici yazılımları.
6	Hayır	Saldırı enflasyonu.
7	Hayır	Hızlı iyileşme ve hata teşhisinin negatif sonuçları.

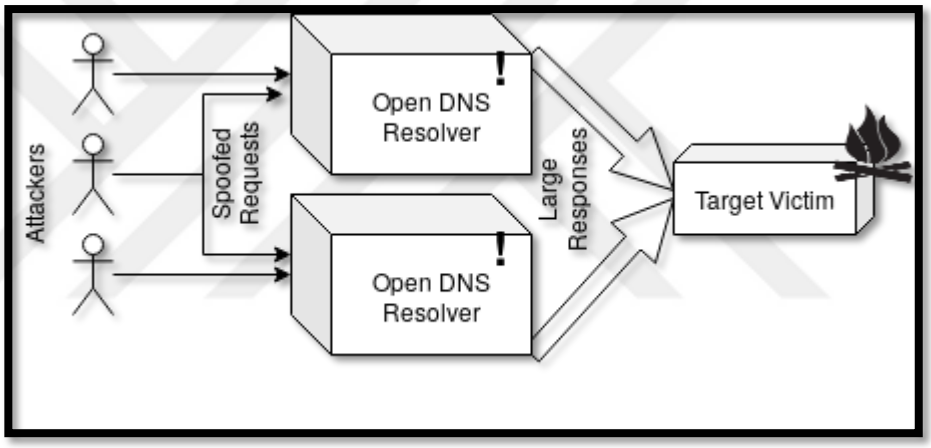
Bu çalışmada ise bazı ağ bilgileri toplanıp, gerçek zamana yakın olarak değerlendirilip, bir DDoS çeşidi olan DNS kuvvetlendirmeli DDoS saldırısı önlenmeye çalışılacaktır. Bir sonraki bölümde DNS kuvvetlendirmeli DDoS saldırılarına genel bir bakış atılacak ve dünyadaki son durum hakkında bilgi verilecektir. IHS Markit tarafından, 23 servis sağlayıcı ile yapılan bir anket sonucu [4], 2018 sonunda bu servis sağlayıcıların 2/3 oranında SDN kullandığını, bunun 2019 sonunda ise %87'ye çıkacağı görülmüştür. Servis sağlayıcılar bu ağ altyapısına yatırım yapmak için iki önemli sebep sunmuşlardır. Bunlar, servisin basitleşmesi otomasyonu servis hızı ve uçtan uca ağ yönetimi olarak belirtilmiştir. Şuradaki [5] çalışmada ise, SDN güvenlik açıkları, saldırıları ve zorluklarının sınıflandırması Tablo 2.2'ye göre yapılmıştır.

Tablo 2.2: SDN güvenlik sınıflandırması.

Güvenlik Çözümleri Kategorileri	**SDN Katmanları / Ara yüzü**	**Güvenlik Önlemleri**	**Simülasyon Ortamı**	**Güvenlik Hedefleri**
Güvenli tasarım	Uygulama katmanı	Erişim denetimi	NOX	Mesuliyet
Güvenlik denetimi	Denetim katmanı	Ulaşılabilirlik	Mininet	Güvenlik uygulaması geliştirme
Güvenlik uygulama politikası	Altyapı katmanı	Bütünlük	Openflow enabled switches	Güvenlik görüntüleme
Güvenlik arttırma	Güney ara yüzü	Gizlilik	Floodlight	Kötücül yazılım koruması
Güvenlik analizi	Kuzey ara yüzü	Sızma tespiti algılama ve engelleme	Open nebula	Güvenli mimari
		Adli destek	OpenVSwitch	DoS/DDoS koruması
		İnkar edilememe	Openflow Standards	Güvenlik duvarı ve IPS geliştirmesi
			Ryu	Hataya dayanıklılık

2.2. DNS ve Kuvvetlendirme/Yansıma Saldırıları

DNS Kuvvetlendirmeli DDoS saldırıları, hedeflenen bir sunucuyu veya ağa, kuvvetlendirilmiş ve yansıtılmış bir trafik yollayarak darboğaza sokma hedefli saldırılardır. DNS yapısının bir özelliğini kullanarak, hedefi (sunucu veya ağ) kullanılmaz hale getirmeyi hedeflemektedirler. DNS sunucularına gönderilen küçük sorguların çok büyük yanıtlar vermesi ve kaynak IP adresi, kurbanın IP adresi yapılarak, kurbanın üzerine çok büyük veri gelmesini hedeflenir. UDP temelli olduğundan, oturuma tabi değildir. Böylece ufak bir sorgudan büyük yanıt elde edilerek kuvvetlendirilmiş, IP adresi saklandığı içinde yansıtılmış bir saldırı haline gelmektedir. Bu saldırının bir şeması Şekil 2.4'te gösterilmiştir.



Şekil 2.4: DNS kuvvetlendirme/yansıtma saldırısı.

Bu saldırı türü temelde yansıtıcı olarak kullanılan DNS sunucularının ANY sorgusuna yanıt vermesi engellenerek çözülebilir. Ancak bazı durumlarda bu sorguya yanıt vermesi gereken sunucular veya yanlışlıkla bu özelliği açılmış sunucular ağ içinde bulunabilirler. Bu durumlarda, ağ yöneticilerinin bir önlem almaları gereklidir. Yansıtıcı olarak kullanılan DNS sunucuna gelen isteklerin toplam boyutunun, verdiği yanıtlarının toplam boyutuna olan oranına kuvvetlendirme faktörü denilmektedir. Bu değer, saldırının büyüklüğü ile ilgili en önemli metriklerden biridir. Ayrıca, gizlenmiş IP adresinin doğruluğu, saldırıyı anlamak açısından bir diğer önemli metriktir. Şekil 2.5'te google.com için yapılan normal bir DNS sorgusu olan A kaydının, yani bir alt alan adına karşılık gelen IP adresi bilgisi görülmektedir. Şekil 2.6'da ise ANY sorgusu yani bir alan adının tüm alt alan adlarının bilgisinin istendiği sorgu görülmektedir. Sorgu ve yanıt arasında 5 kat büyüklük farkı vardır.

```
;ANSWER
google.com. 299 IN A 173.194.222.113
google.com. 299 IN A 173.194.222.101
google.com. 299 IN A 173.194.222.138
google.com. 299 IN A 173.194.222.102
google.com. 299 IN A 173.194.222.100
google.com. 299 IN A 173.194.222.139
```

Şekil 2.5: DNS için A kaydı sorgusu.

```
;ANSWER
google.com. 299 IN A 173.194.222.139
google.com. 299 IN A 173.194.222.100
google.com. 299 IN A 173.194.222.113
google.com. 299 IN A 173.194.222.138
google.com. 299 IN A 173.194.222.101
google.com. 299 IN A 173.194.222.102
google.com. 299 IN AAAA 2a00:1450:4010:c0b::66
google.com. 21599 IN NS ns3.google.com.
google.com. 21599 IN NS ns1.google.com.
google.com. 21599 IN NS ns4.google.com.
google.com. 21599 IN NS ns2.google.com.
google.com. 299 IN TXT "docusign=1b0a6754-49b1-4db5-8540-d2c12664b289"
google.com. 299 IN TXT "facebook-domain-verification=22rm551cu4k0ab0bxsw536tlds4h95"
google.com. 299 IN TXT "globalsign-smime-dv=CDYX+XFHUw2wml6/Gb8+59BsH31KzUr6c1l2BPvqKX8="
google.com. 299 IN TXT "v=spf1 include:_spf.google.com ~all"
google.com. 299 IN TXT "docusign=05958488-4752-4ef2-95eb-aa7ba8a3bd0e"
google.com. 599 IN MX 50 alt4.aspmx.l.google.com.
google.com. 599 IN MX 20 alt1.aspmx.l.google.com.
google.com. 599 IN MX 10 aspmx.l.google.com.
google.com. 599 IN MX 40 alt3.aspmx.l.google.com.
google.com. 599 IN MX 30 alt2.aspmx.l.google.com.
google.com. 21599 IN CAA 0 issue "pki.goog"
google.com. 59 IN SOA ns1.google.com. dns-admin.google.com. 281030299 900 900 1800 60
```

Şekil 2.6: DNS için ANY kaydı sorgusu.

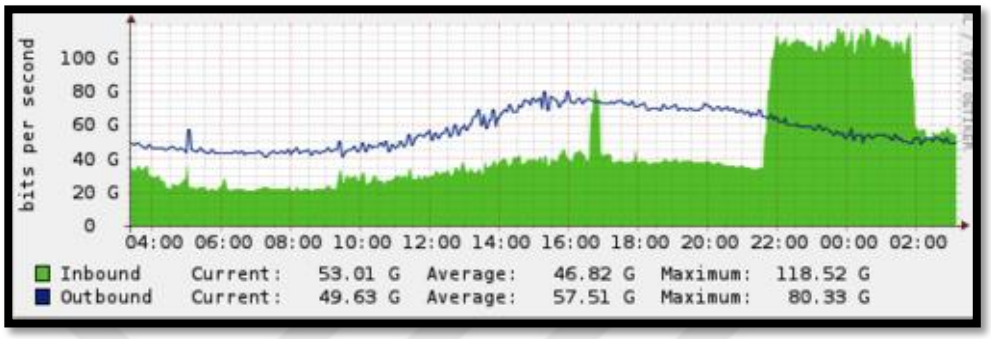
Bu saldırı türünün tespiti ve tahmini için birçok metot çalışılmıştır. Şu çalışmada [6], özellikle geleneksel ağlarda yapılan çalışmaların bir listesi bulunmaktadır. Bunların bir kısmı, saldırı örüntü korelasyonu, tarihsel olarak tutulmuş IP adresi listeleri, gelen ve giden paketlerin boyutlarının karşılaştırılması, paket puanlama, tekrarlanan paketlerin izlenmesi, gelen ve giden paketlerin içeriklerinin incelenmesi, IP adresi gizleme önleme yöntemleri, oyun teorisi ile saldırı tahmin etme, saldırıyı algılamak için bal küpü kullanımı gibi çalışmalardır. SDN üzerinde yapılan çalışmalar bir sonraki bölümde detaylı incelenecektir.

Bu saldırı türü, yansıtıcı olarak kullanılan DNS sunucularının ANY türü sorgulara yanıt vermesi yasaklanarak engellenebilir. Ancak sunucuların bu sorguları yanıtlamaları gerektiği veya bu özelliğin yanlışlıkla açıldığı durumlarda ağ yöneticilerinin harekete geçmesi gerekmektedir. Bu saldırı türündeki en önemli metrik, yanıt paketleri ve sorgu paketleri arasındaki orandır. Bu orana Kuvvetlendirme Faktörü(Amplification Factor, AF) denir. Şuradaki [7] çalışmaya göre DNS ve başka UDP temelli uygulamaların oluşturduğu kuvvetlendirmeleri ve değerleri Tablo 2.3 'teki gibidir.

Tablo 2.3: Uygulamaların port ve AF değerleri.

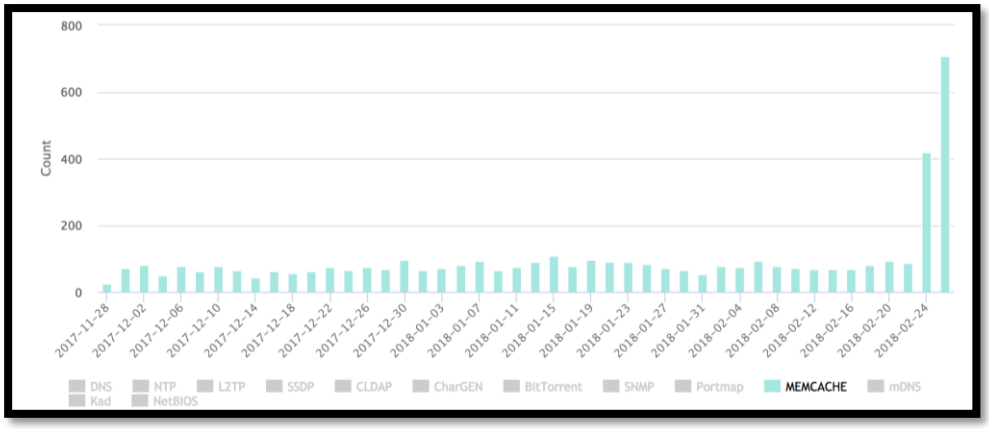
Protocol	**Port**	**AF**
SNMP	161	6.3
NTP	123	556.9
DNS ns	53	28
DNS or	53	54
NetBios	127	3.8
SSDP	1900	30.8

2013 yılında Spamhaus'a yapılan saldırı (Şekil 2.7) [8] bir DNS saldırısıydı. Saldırı boyutu 2016 'da 600 Gbps'a kadar çıkmıştı. Sonuç olarak Open Resolver Project [9] ortaya çıkmış ve konuyla ilgili, open-resolver DNS sunucularının tespiti, nasıl kapatılacağı, sunucu türleri için yamalar hazırlanması, bilgilendirme, yanıt sınırlaması (Response Time Limit) yamalarının hazırlanması gibi çalışmalar yapıldı.



Şekil 2.7: Spamhaus'a yapılan saldırının bir grafiği.

Techrepublic'teki yayına göre [10] 2018'den beri DNS kuvvetlendirme saldırıları %1000 artmıştır. Tüm saldırıların %35'inden fazlası ABD veya Çin kaynaklı, Vietnam ve Rusya üçüncü ve dördüncü sıradadır. Cloudflare'in paylaştığı [11] ve şekil 2.8'de gösterilen grafiğe göre, UDP tabanlı birçok kuvvetlendirme saldırısı bulunmaktadır. Ayrıca memcache uygulamasının bir açığından faydalanan saldırganların, 2018'de saldırıların büyük bir yüzdesine neden olduğu görülmüştür. Bu rapordan esinlenerek, başka UDP tabanlı kuvvetlendirme saldırılarına çözüm olma hedefi de koyulmuştur.



Şekil 2.8: Kuvvetlendirme saldırıları ve kullanılan uygulamalar.

3. KONU İLE İLGİLİ ÇALIŞMALAR

Bu konuda hem geleneksel ağlarda, hem de SDN tabanlı ağlarda oldukça fazla çalışma yapılmıştır. DDoS tespiti, DNS kuvvetlendirme saldırılarının önlenmesi ve azaltılması ile ilgili çeşitli yaklaşımlar sunulmuştur. Öne çıkan yöntemler, zaman serisi temelli çözümler, İstatistiksel entropi yöntemleri, desen dağılımlarına dayalı makine öğrenmesi (ML) algoritmaları, DNS sorgu geçmişi eşleştirme yöntemleri vb.

Dharma et al. [12], SDN denetleyicisinde zaman tabanlı bir çözüm sunar. Yöntem, yoğun trafiği gözlemlemeyi, çıkan desenleri kümelemeyi ve eşik temelli bir azaltma işlemi öne sürmektedir. Akışı toplayan bir mekanizma ile denetleyici tarafından gönderilen paketleri istatistiksel bir yöntem ile analiz etmektedir.

K. Kalkan et al. [13] SDN üzerinde DDoS saldırılarının tespiti ve önlenmesi için istatistiksel entropi yöntemleri kullanmışlardır. Bu yöntem ML algoritmalarına kıyasla sistem yükünü azaltır. Ayrıca istatistiksel yöntem sayesinde, önerilen prosedürler bilinmeyen saldırı türlerini de tespit edebilir ve hafifletebilir. Bu bağlamda bir önceki çalışmalarında [14], akıllı ağ anahtarı tabanlı bir istatistiksel modeldir. Tüm paketler incelenir ve nitelik değerleri ile skorları belirlenmektedir.

R. Wang et al. [15], belli bir süre boyunca toplanan, istatistiksel özelliklere dayalı profiller üretmek ve paketleri bu profillerle karşılaştırdıktan sonra saldırıya ait paketleri bulmaya çalışan istatistiksel bir entropi modeli kullanmıştır. Fakat bu yöntem kurbanı veya şüpheli makineleri bulmaz ve onları engelleyemez.

L. Li et al [16], ağ paket başlıklarındaki desenlerin dağılımlarını hesaplayarak, bir saldırı tespiti algoritması ortaya koymuştur. Paket sınıflandırması yerine kümülatif trafik entropisi hesaplamıştır ve şüpheli olan trafiği tespit etmektedir. Yöntem önceden tanımlanmış eşik değerlerini kullanmak yerine, anomali tespiti yapmaktadır. Anomali bir süre devam ederse, trafik anormal olarak işaretlenmektedir. Temel olarak kaynak IP adresi değişimine bakmaktadır. Bir önceki çalışmasına geliştirme olarak, iki gelişmiş tespit metodu eklemiştir. Bunlar sırasıyla kümülatif entropi ve zamandır.

Entropi tabanlı bir diğer yaklaşım K.Kumar t al. [17], dağıtık bir entropi hesabı kullanmıştır. Kaynak IP adresi entropisi ile Chi-square yöntemini kullanmıştır. Ancak bu noktada bellek ve hesaplama yükü tek bir noktada toplanmıştır.

C. Jin et al. [18] IP başlığındaki TTL değerinden Hop sayısını bularak ve bunları kaynak IP adresleriyle eşleyerek Hop Count Filter (HCF) geliştirmiştir. Daha sonra HPC kullanarak sahte IP adreslerine karşı bir savunma sistemi tasarlamıştır. Burada sezgisel olarak kaynak IP adresi aynı olan paketleri TTL değerlerinin de aynı veya benzer olması üzerinedir. Ancak yansıtma yapan makineye gelen isteklerin kaynak IP adreslerinin sayıları arttıkça HCF için tutulan değerler artacaktır. Bu durum çok fazla kaynak tüketimine neden olacaktır.

Chih-Chieh Chen et al. [19], DRDoS saldırıları için makine öğrenmesine dayalı bir tespit metodu sunmaktadır. Sistem, SDN içindeki DNS/NTP paketlerini bir SVM sınıflandırıcısı ile kategorize eder ve kuvvetlendirme saldırısı olduğunu düşündüğünde saldırıyı bloklar. Sistemi sadece DNS kuvvetlendirme saldırısı ile eğitmesine rağmen, NTP temelli saldırı için de çalıştığı görülmüştür.

Oldukça fazla, önceden tanımlanmış eşik değerlerini temel alan sitemler önerilmiştir. Sflow ile toplanan verilerin önceden tanımlanmış eşik değerleri ile karşılaştırılmasını sağlayan bir çalışma [20] yapılmıştır. Ayrıca, D. Huistra et al. [21], DNS paket boyutlarının hesaplanması ve eşik değerlerine bakarak saldırı tespiti sunan bir yöntem ortaya sunmuştur.

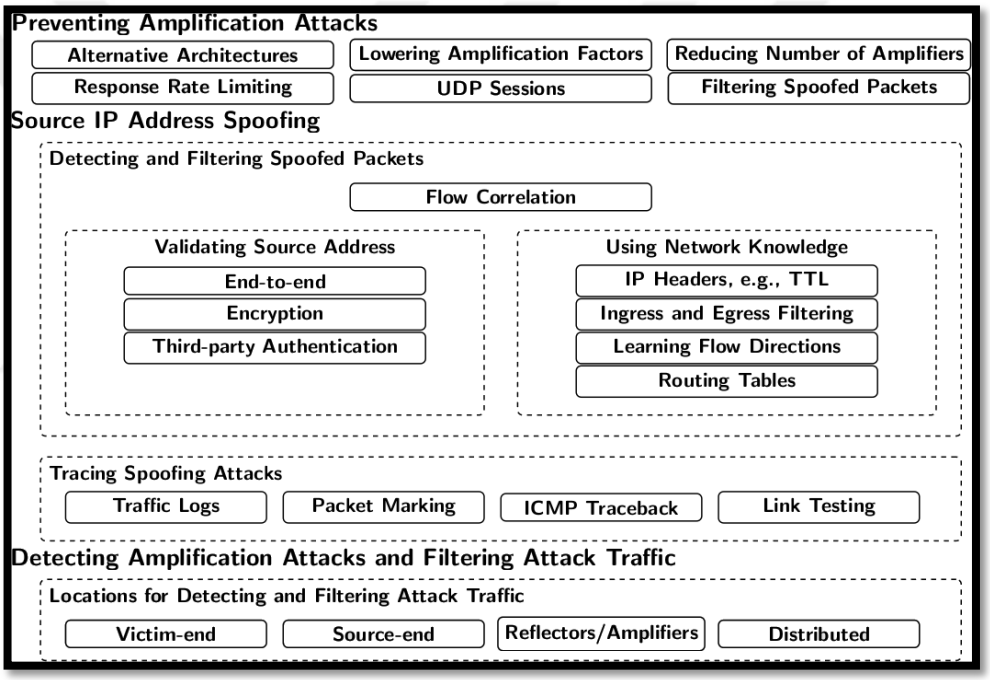
J. Zeng et al. [22], ticari kullanıma hazır (COTS), adaptif korelasyon analizi yöntemi ile gerçek zamanlı bir DDoS saldırısı engelleyici sistem tasarlamıştır. RADAR ismini verdiği bu sistem, yenilik olarak şüpheli analizleri tespit için yaptığı korelasyon sadece ağ anahtarları üstünden yapmasıdır.

G. Kambourakis et al. [23], tarafından sunulan çalışma, DNS sorgu ve yanıtlarını birebir eşleyerek DNS kuvvetlendirme saldırıları için adil bir çözüm sunmaktadır. Şüpheli bir paket geldiğinde, sayaç bir arttırılır ve belirtilen eşik değerine geldiğinde ise saldırı uyarısı verilir. Buradaki problem çok büyük miktarda verinin saklanması gerektiğidir.

VAVE [24], sanal kaynak adres onayı yapmaktadır. DDoS önlemek için akış girdilerini, filtreleme ve adres onayı araştırmak için NOX denetleyicisini geliştirmiştir. Gelen tüm paketleri doğrular ve kararlar alır. Böylece kaynak IP adresini gizleyen DDoS saldırıları için geliştirmeler yapmıştır.

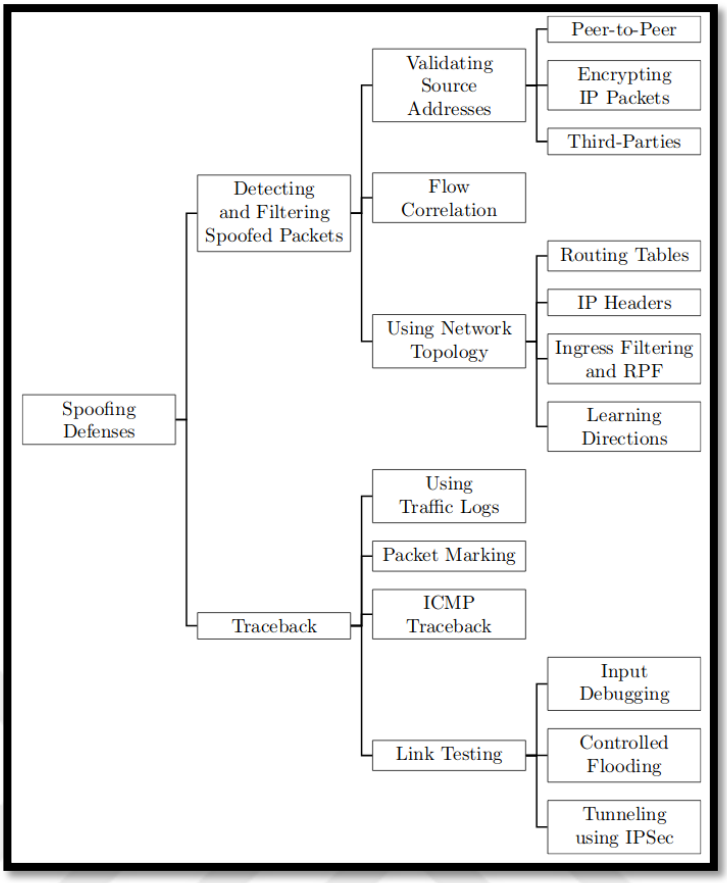
Bohatei [25], sanal yönlendiricileri izler, trafik kurbana doğru aktığında ve önceden tanımlanmış bir eşiğe vardığında DDoS saldırılarını tespit eder. Yapılan deneyler, ölçeklenebilir (500 Gbps saldırılar gelmekte), hassas (bir dakika içinde saldırıyı hafifletme) ve dinamik saldırılara karşı esnek olduğunu ortaya koymuştur. Ancak sanal makine çalıştırmasından dolayı, taşıyabileceğinden daha fazla trafik geldiği durumlarda etkili değildir.

Bir başka araştırma [26] ise, DRDoS ile gelen kuvvetlendirmeyi önleme, kaynak IP adresi sahtekarlığını tespit etme ve filtreleme, savunmanın yeri ile ilgili bir sınıflandırmadır ve Şekil 3.1'de gösterilmektedir. Yine aynı araştırmada IP adresi gizlenen saldırılardaki defans mekanizmaları Şekil 3.2'de sınıflandırılmıştır.



Şekil 3.1: DRDoS sınıflandırması.

Bir sonraki bölümde daha ayrıntılı bahsedilecek olan bu çalışmada ise, DNS istek ve yanıtlarındaki büyüklüğün oranı ve IP başlığında bulunan TTL değerindeki değişimi, geçmişe ait verileri tutmadan, önceden belirlenmiş eşik değerleri ile karşılaştırarak, saldırıları tespit eden, engelleyen, hafif (lightweight) ve reaktif (reaktif) bir sistem tasarlanmıştır. Saldırı bittiğinde normal haline dönmesiyle de, uyumlu (adaptive) bir sistem olarak adlandırılabilir.



Şekil 3.2: IP adresi gizlenen saldırılar için defans sınıflandırılması.

Bu bölümde üstünde durulan çalışmalarda, 2 farklı başlığın daha fazla rol oynadığı görülmüştür. Bunlar Amplification Factor (AF) ve Hop Count (HC) metrikleridir. AF için, DRDoS saldırılarının temel metriği denebilir. Birçok çalışmada kullanılmıştır. Ancak AF için hangi değeri için saldırı olduğu belli değildir. AF yüksek ve saldırı gerçekleşmiyor olabilir. Saldırı aynı zamanda IP adresi gizlenerek yapıldığından, AF tek başına yeterli değildir. DRDoS saldırısının bu özelliği de dikkate alınmalıdır. Bunun içinde HC değeri önemlidir. HC değerindeki değişiklikler bu saldırının IP adresi gizlenen bir saldırı olduğu üzerine önemli bir bilgi vermektedir. Ancak Hop Count Filter üzerine çokça çalışılmasına rağmen, özellikle kaynak tüketimi eleştirilmektedir. Farklı ağaç yapıları, değişik bellek yerleşimleri, farklı dosya yazım biçimleri, yeni gerçeklemeler, işletim sistemi çekirdeği gerçeklemesi, tarihi verinin ne kadar tutulacağı, önbellek sistemleri gibi geniş çaplı çalışılmış bir konu olmasına rağmen, yüksek kaynak kullanımı devam etmektedir. Bu eleştiriler ölçüsünde bir sonraki bölümde, bahsedilen başlıklar daha ayrıntılı incelenecektir.

4. ÖNERİLEN YÖNTEM - YARASA

Bu bölümde saldırı tespiti ve engellenmesi ile ilgili mekanizmalar detaylı olarak açıklanacaktır. Özet olarak bu çalışmada, SDN üzerinde DNS DRDoS saldırılarına karşı bir sistem geliştirilmiştir. SDN tabanlı bir ağda bir veya daha fazla DNS sunucusu ve kurban bilgisayarın bulunduğu varsayılmaktadır. DNS sunucusu yansıtıcı ve kuvvetlendirici olarak kullanarak, kurban üzerinde büyük bir UDP trafiği yaratılacaktır. Saldırının tespiti ve hafifletilmesi ayrı ayrı incelenecek ve tespit sırasında iki aşamalı bir yöntem uygulandığı görülecektir. Ardından engelleme sağlanacaktır. Ayrıca, DNS sunucularının yerini gösteren bir ön işlem bulunmaktadır. Saldırının tespiti için iki metrik hesaplanacak ve gözlemlenecektir. Bunlar, Kuvvetlendirme Faktörü (Amplification Factor, **AF**) ve TTL başlığı üzerindeki değişimi temel alan Durak Sayısı Değişimi (Hop Count Variation, **HCV**). Bu iki metriğin zaman içindeki değimi izlenerek saldırı tespiti yapılacaktır. Hafif bir sistem hedeflendiğinden, paket içeriği inceleme (Deep Packet Inspection, DPI) ve filtreleme yapılmayacaktır. TTL ile Herhangi bir tarihsel veri tutulmadığından sistem tepkiseldir (Reactive). Ayrıca saldırı bittiğinde normale dönebildiğinden uyarlanırdır (Adaptive).

4.1. Kuvvetlendirme Faktörü (AF)

DNS sunucularına gelen isteğin boyutu ile yanıtın boyutu arasındaki oran Kuvvetlendirme Faktörü (AF) olarak bilinmektedir [25] [19]. Özyinelemeli DNS sorgusuna verilen yanıtın, A veya CNAME gibi bir sorgunun yanıtından daha büyük olduğu bilinmektedir [27]. AF için genellikle aşağıdaki denklem kullanılmaktadır.

$$AF_1 = \Sigma \text{ (response)} / \Sigma \text{ (request)} \tag{4.1}$$

$$AF_2 = \bar{x} \text{ (response)} / \bar{x} \text{ (request)} \tag{4.2}$$

AF_1, yanıtın büyüklüğünün sorgunun büyüklüğüne olan oranıdır. AF_2 ise yanıtların kümülatif büyüklüğünün, sorgularınkine olan oranıdır. Bu metrikteki artış olası bir saldırının özelliklerinden biridir [28].

Bununla birlikte, bu sorgunun cevabının küçük olduğu, TXT, NS, MX kayıtlarının yanıtlarının büyük olduğu veya DNSSEC etkin olduğu durumlarda, AF saldırıyı anlamak için yeterli olmayabilir [29]. Literatürde tanımlanan iki farklı AF vardır. Bant genişliği kuvvetlendirme faktörü (BAF), talebin UDP yükü sayısına kıyasla bir AF verdiği UDP yükünün sayısını ifade eden bant genişliği çarpanıdır. Paket kuvvetlendirme faktörü (PAF) ise, bir kuvvetlendiricinin yanıt verdiği IP adresi paketlerinin sayısını referans alan bir paket çarpanıdır. Bu çalışmada, BAF olarak DNS ANY sorguları kullanılmıştır. AF, bir saldırının kuvvetlendirme özelliğini anlamak için kullanışlıdır. Ancak, saldırının türünün dağıtık olanı aynı zamanda bir IP gizleme tekniği içermektedir. Bu teknik AF dışında başka bir bilgi ile anlaşılabilirdir.

4.2. Durak Sayısı Değişimi (HCV)

IP paket başlığındaki (Şekil 4.1) TTL değeri, kaynak makineden, hedef makineye giderken sabit bir değer olarak belirlenerek, paketlerin sonsuza dek yönlendirilmemesi için kullanılmaktadır. TTL, sahte paketlerin tespiti için önemli bir başlıktır. Rotalar değişse bile, durak sayılarında önemli değişimler olmaz veya bir kere olur. IP başlığındaki TTL başlığı için iki önemli bilgi vardır.

bit offset	0-3	4-7	8-13	14-15	16-18	19-31
0	Version	Internet Header Length	Differentiated Services Code Point	Explicit Congestion Notification	Total Length	
32	Identification				Flags	Fragment Offset
64	Time to Live		Protocol		Header checksum	
96	Source IP Address					
128	Destination IP Address					
160	Options (if Header Length > 5)					
160 or 192+	Data					

Şekil 4.1: IP paket başlığı.

Birincisi TTL başlangıç değeri, ikincisi ise geçtiği her durak için olan azalmadır. TTL, IP paketinin yaratıldığı makine ve işletim sistemine göre değişmektedir [30] ve Tablo 4.1 'de UDP varsayılan değerlerinin, işletim sistemlerine göre örneği gösterilmiştir. Kaynak adresini gizleyen saldırganlar, sömürülen istemcilerin, işletim sistemlerinin farklı olması nedeniyle, makinenin IP adresi farklı olabilmektedir.

Tablo 4.1: İşletim Sistemleri için TTL başlangıç değerleri.

İşletim Sistemi	**TTL Başlangıç Değeri**
Linux (kernel 2.4 and 2.6)	64
FreeBSD	64
Windows XP, 7 and Server 2008	128
MacOS X (10.5.6)	64
Cisco Router (IOS 12.4)	255

Şu [31], çalışmada belirtildiği gibi, TTL değeri kullanılarak Durak Sayısı (Hop Count, HC) belirlenir. HC ile belli bir pencere aralığındaki farklı HCV değerlerinin sayısı hesaplanır ve bu değer saldırıda bir IP adresi gizleme olduğunun göstergesidir. Bu değere, Durak Sayısı Değişimi (HCV) denmektedir ve temel algoritması Şekil 4.2 'de gösterilmiştir.

Require: $ttl > 0$
1. **if** $ttl < 33$ **then**
2. $\quad hc = 32 - ttl$
3. **else if** $(ttl) < 65$ **then**
4. $\quad (hc) = 64 - ttl$
5. **else if** $96 < ttl < 129$ **then**
6. $\quad hc = 128 - ttl$
7. **else if** $224 < ttl < 256$ **then**
8. $\quad hc = 255 - ttl$
9. **else**
10. $\quad$ **return** $hc - 1$
11. **end if**
12. **return** hc

Şekil 4.2: TTL verisinden HC verisini elde etme algoritması.

4.3. Saldırı Tespiti

Başlangıçta, ağdaki DNS sunucularının yerlerini belirlemek için, sistem belirli aralıklarla taranır. Bu aşamada, bağlantı noktası 53'e giden ve gelen paketler 7. katmana kadar çözülür ve bunun bir DNS sorgusu olup olmadığına karar verilir. Bağlantı noktası 53, DNS sunucuları tarafından varsayılan olarak kullanılsa da isteğe bağlı olarak başka bir uygulama tarafından kullanılabilmektedir. Böylece 53 numaralı bağlantı noktası üzerinden iletişim kuran ve DNS olmayan sunucular izlenmezler. Bu iki aşamalı tespit aşamasına geçmeden önce ve sürekli olarak yapılır. Çünkü bir sonraki aşamada metrik hesaplama hemen başlayacaktır. Gerçekte, bu saldırı türü hem kuvvetlendirme hem de IP adresi gizleme davranışlarını içerir. Bu nedenle iki aşamalı bir yöntem önerilmiştir. Son olarak, bundan sonra bu sisteme YARASA (Yet Another Reflection/Attack Security Application in SDN) ismiyle anacağız. YARASA, paketleri 4. katmana kadar çözer, uygulama katmanına kadar gidip paket içeriklerine bakmaz.

4.3.1. Aşama 1: Kuvvetlendirme Faktörü İzleme

Bu aşamada, tespit edilen DNS sunucularına gelen isteklerin ve giden yanıtların denetleyici aracılığıyla toplanması ve AF hesaplaması yapılmaktadır. AF değerinin artması, olası bir saldırının gerçekleşiyor olması anlamına gelmektedir. DNS kuvvetlendirmeli saldırılar genellikle, ANY sorgusunu kullanırlar. Bununla birlikte AF değeri, DNSKEY, TXT, NS, MX gibi başka sorgular yapılarak ta arttırılabilir. Bu nedenle, AF değerinin artması, saldırının hemen başladığı anlamına gelmez. Bu sorunu gidermek için olan metod Aşama 2'de anlatılmıştır.

Bu aşamada incelenen AF için ayarlanması gereken 2 eşik değeri vardır. Alt eşik ve Üst eşik. Alt eşik aşıldığında YARASA, normal sorguları düşürmemek için ikinci aşamaya geçer. Üst eşik aşıldığında ise, ikinci aşama atlanır ve doğrudan engelleme/azaltma bölümüne geçilir.

4.3.2. Aşama 2: Durak Sayısı Değişimi İzleme

Bu aşamada, istemcinin DNS isteklerini yaptığı IP paketinin başlıklarındaki TTL değerlerinin sunucudaki yüksek AF değeri ile birlikte değişimi incelenir. HCV değeri belirtilen eşik değerinden yüksekse, önleme aşaması başlatılır. Aksi takdirde hiçbir şey yapılmaz ve Aşama 2, Aşama 1 'den yeni bir tetikleme beklemeye devam edecektir. Bu, AF değerinin Aşama 1'de yüksek olduğu anlamına gelir ancak DNS kuvvetlendirme saldırısı olduğu anlamına gelmez.

HCV hesabı, sürekli yapılmaz. Sadece Aşama 2 tetiklendiğinde yapılır. Böylece tüm istemciler için sürekli HCV hesaplanıp kaydedilmez. Bu, aşırı hesaplama kaynağına ihtiyacı ve IP-TTL eşleştirme gibi büyük bir veri deposunu ortadan kaldırır. Çünkü her istemci IP adresi için bir IP-TTL eşleştirme tablosu tutulmalıdır. Ancak, YARASA bu hesaplamayı yalnızca Aşama 2'ye geçmiş DNS istemcileri için gerçekleştirmektedir. Eğer AF değeri 2 eşik arasında kalan bir saldırı varsa ve HCV değişmiyorsa, olası bir saldırı devam edecektir. Ancak vereceği hasar belirlenen eşik değerleri ile ölçeklenebilir. Burada Sistem yöneticisinin doğru değerleri ayarlaması kritik noktadır. Ayrıca HCV değişmiyorsa, saldırı büyük ihtimalle bir DoS saldırısıdır ve yaratacağı hasar DDoS saldırılarına göre çok düşüktür.

Sonuç olarak, bu iki metrik gerektiği koşullar sağlandığında bir zaman serisi veri tabanına yazılarak, gerekli pencere boyutlarında sorgular yapılacaktır. Bu sorgular sonucunda n kere saldırı olduğuna karar verilirse, Saldırı önleme/azaltma bölümü tetiklenir. Yine aynı şekilde n kere HCV değişmiyorsa saldırı bitmiş demektir. Bu, sistemi reaktif yapan özelliktir. YARASA, AF değeriyle kuvvetlendirmeyi, HCV değeri ile yansımayı anlamaya çalışmaktadır. Burada 2 aşamalı bir AF eşik değerleri belirleyerek hafif (lightweight) bir sistem oluşturulmuştur. Bir pencere içindeki farklı HC değerlerinin sayısı bize HCV değerini verir. En son olarak, kaç pencere boyunca bakılıp, saldırı olup olmadığına karar verme değeri Window Count (WC) belirlenmeli ve Pencerenin süresi Window Time (WT) değeri ayarlanmalıdır. Bu değerler sistemin ne kadar çevik olacağının da ayarlanmasını sağlamaktadır. Çeviklik daha fazla kaynak tüketimi anlamına da gelmektedir.

4.3.3. Saldırı Önleme/Azaltma

DNS kuvvetlendirme saldırılarının azaltılması ve engellenmesi için US-CERT [32] ve Open Resolver Project'in [9] tavsiye ettiği yöntemler bulunmaktadır. Bunlar;

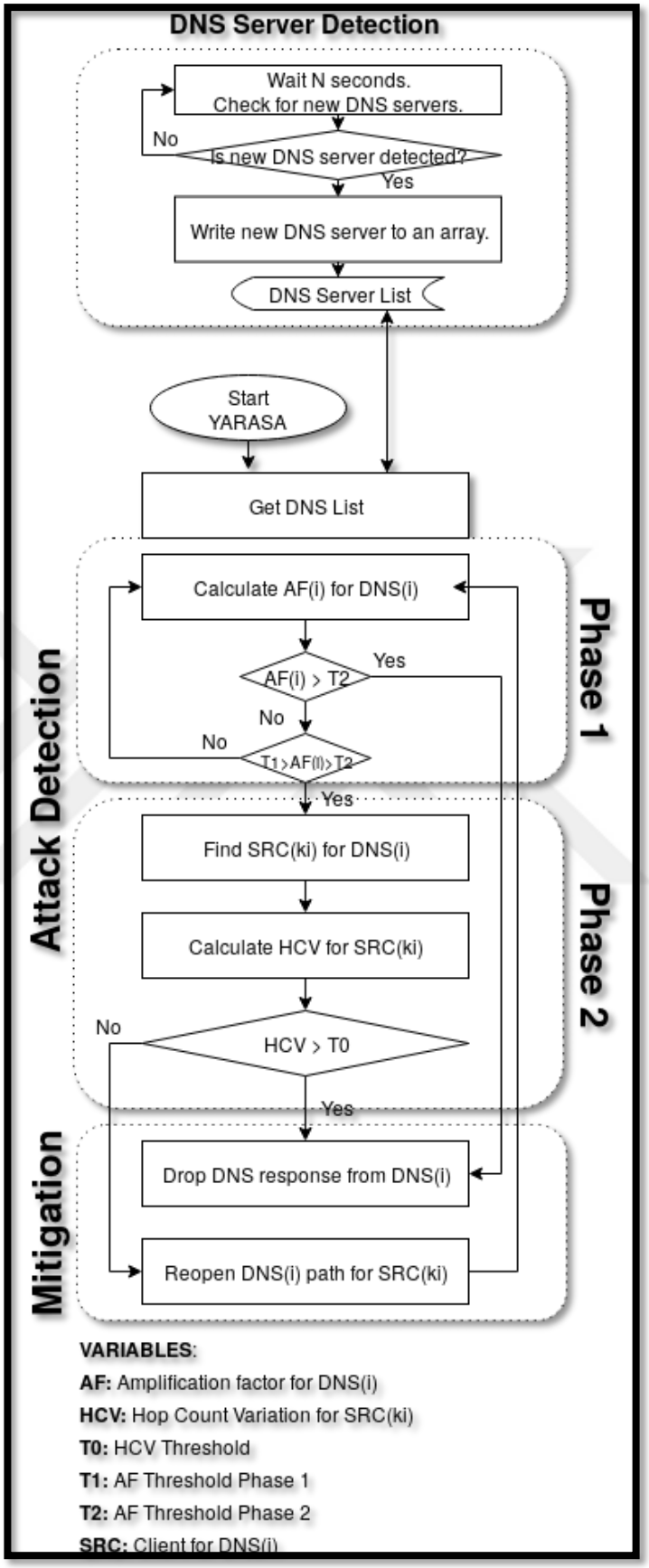
- Kaynak IP adresi doğrulama (Genellikle ISP'ler tarafından yapılabilirler.)
- DNS sunucularının yineleme özelliğini kapatma veya sınırlı erişim.
- DNS sunucusunun vereceği yanıtları sınırlama.

Tavsiye edilen olarak, yineleme özelliği gerekmediği takdirde kapalı gelmelidir. Açılacaksa da gerekli olan IP adresleri için açılmalıdır. Yanıtları sınırlama, darboğaz olmaması için mantıklı olabilir ancak pratikte gerçekten onu kullanacak olan istemcilere sıra gelmeyecektir. Her bir istemci için yapılacak sınırlama çok fazla kaynak isteyeceğinden, bu çalışmada saldırı önleme/azaltma olarak DNS sunucusunun yanıtlarını engelleme seçilmiştir. Bu şekilde saldırgan bulunamayacak (başka bir problemin) ancak yansıtıcı olarak kullanılan DNS sunucusu bant genişliği yaratmayacak, kurbanın hayatına devam edecek ve ağda darboğaz yaratamayacaktır.

YARASA, önleme/azaltma aşamasını başlattıysa, yansıtıcı olarak kullanılan bir DNS sunucusu var demektir. Kurbana giden trafiği azaltmak için, DNS sunucusunun yanıt vermesi engellenir. Uygulamada, DNS sunucusu yanıt verse bile, yanıtlar ilk ağ anahtarı üzerinde düşürülecektir. Sonuçta, gerekli olan FLOW_MOD girdisi tüm ağ anahtarlarına gönderilir. Bu yöntem, DNS sunucusu tarafından oluşturulan tüm yükseltilmiş yanıtları ağdan düşürecektir. Bu, tüm Open Resolver DNS sunucularının, önerildiği gibi [32] kapatılmasını temsil eder. YARASA için örnek bir yapılandırma Şekil 4.3'te görülmektedir. Şekil 4.4, YARASA'nın bir akış şemasıdır.

```
[yarasa]
name=yarasa_dns
port=53          ; Port for application
t0=5             ; HCV threshold
t1=6.5           ; AF threshold 1
t2=20            ; AF threshold 2
wt=1s            ; Window time
wc=3             ; Window count
;is_adaptive=true
;mitigation_strategy=drop
```

Şekil 4.3: Örnek YARASA yapılandırması.



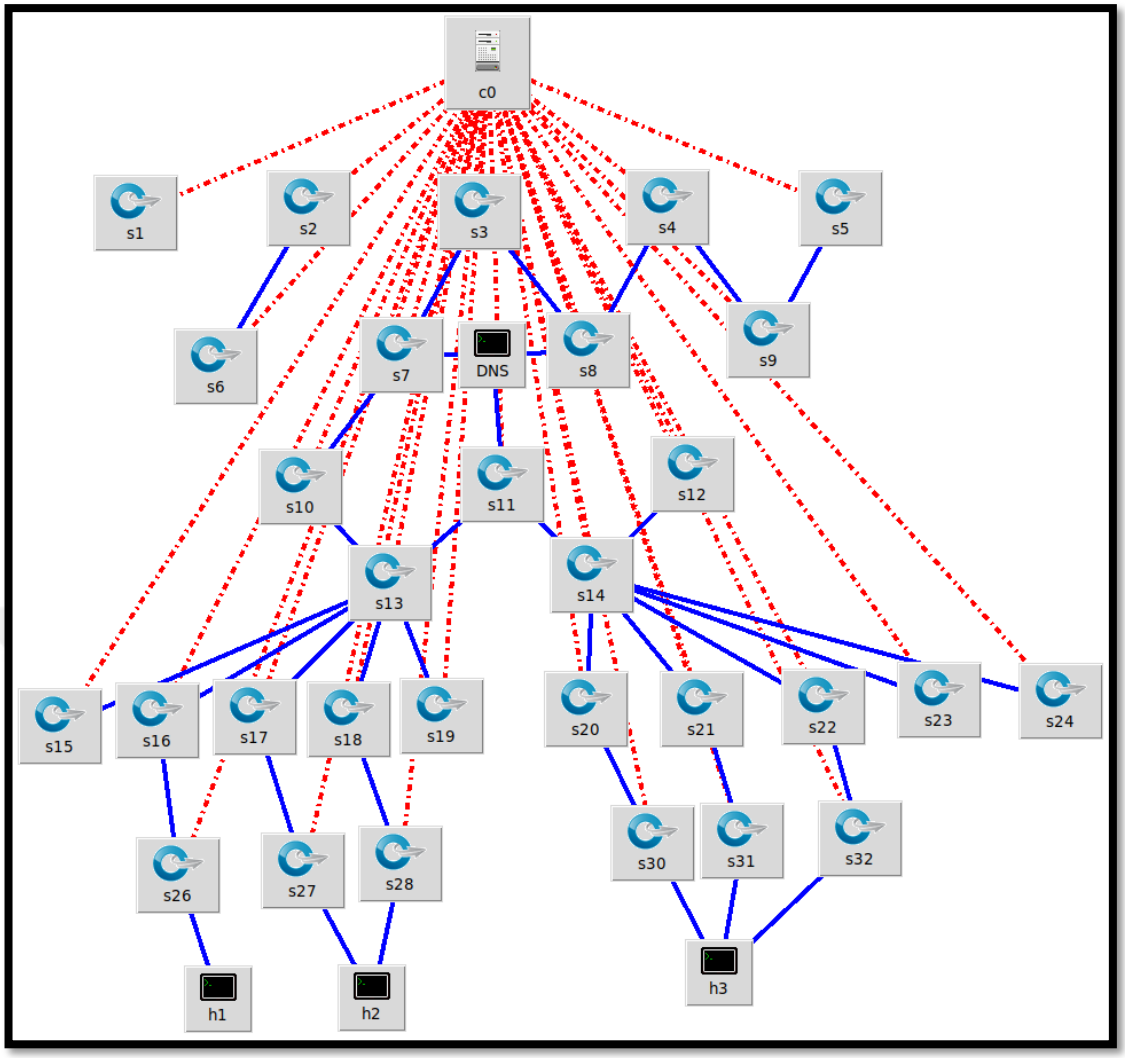
Şekil 4.4: YARASA akış şeması.

5. BENZETİM VE DENEYLER

Bu bölümde, algoritmanın altyapısı ayrıntılı olarak açıklanmaktadır. Sistem gerçek hayat verileri kullanılarak oluşturulan trafiğe karşı test edilecektir. Sistemin tepkisi ve saldırılara karşı etkinliği test edilecektir. Sistemin DNS kuvvetlendirme saldırılarına karşı performansını anlamak için AF ve HCV değerleri üzerinde durulmuştur.

5.1. Altyapı ve Topoloji

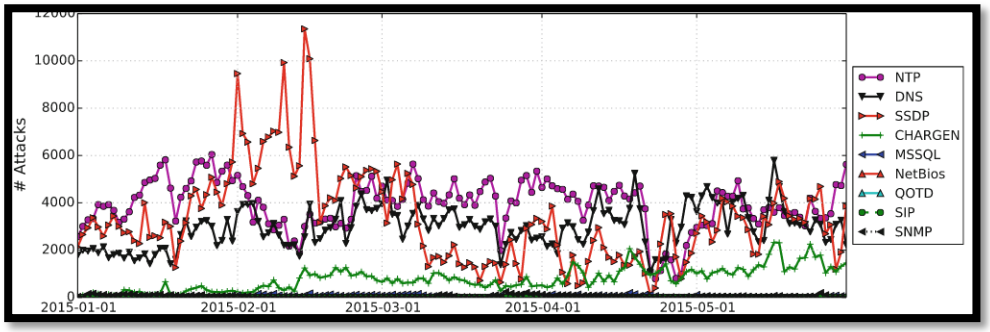
İlk olarak, mininet ve OpenvSwitch ağ altyapısı ve topolojisinin oluşturmak için kullanılmıştır. Ayrıca bu sayede topoloji görselleştirilmiştir. Openflow desteği sayesinde hızlıca denetleyiciye bağlanılmıştır. SDN denetleyicisi olarak RYU kullanılmış ve programlamak için Python dilinin ara yüzü kullanılmıştır. RYU'nın varsayılan olarak gelen python kütüphanesindeki zenginlik sayesinde, istenilen yapı kolaylıkla sağlanmıştır. DNS sunucusu olarak neredeyse bir endüstri standardı olan Bind9 kullanılmıştır. Paket üretmek, manipüle etmek ve kullanmak için Scapy kütüphanesi kullanılmıştır. Denetleyici üzerinden kullanılacak olan veri toplama aracı, verileri bir Time Series veri tabanı olan Influxdb'ye yazmıştır ve anlık olarak grafiksel izleme için aynı aileden olan Chronograph kullanılmıştır. AF ve HCV değerlerine yönelik sorgular, Influxdb üzerinden hesaplanmış ve RYU'nun OpenFlow ara yüzü ile gerekli önleme/azaltma işlemleri yapılmıştır. PCAP analizinde wireshark, termshark ve tshark kullanılmıştır. Özellikle pencere hesaplamaları için Python betikleri kullanılmıştır. Tüm bu altyapı, bir Linux dağıtı olan Debian üzerinde çalıştırılmıştır. Kullanılan topolojinin temsili grafiği, 5.1'de gösterilmiştir. Tüm altyapı tasarlanırken, özgür yazılımlar kullanılmıştır. Böylece çalışmanın tüm gerçeklemeleri de kolayca başka araştırmacılar ile paylaşılabilecektir. Kullanılan tüm araçların özgür yazılım olmasının yanında, YARASA için yazılmış tüm kodlar da bir özgür lisans ile lisanslanacaktır. Böylece veri setine sahip olan her kişi, paylaşılan kodu tekrar tekrar çalıştırıp, kendi çalışmasıyla karşılaştırabilecektir.



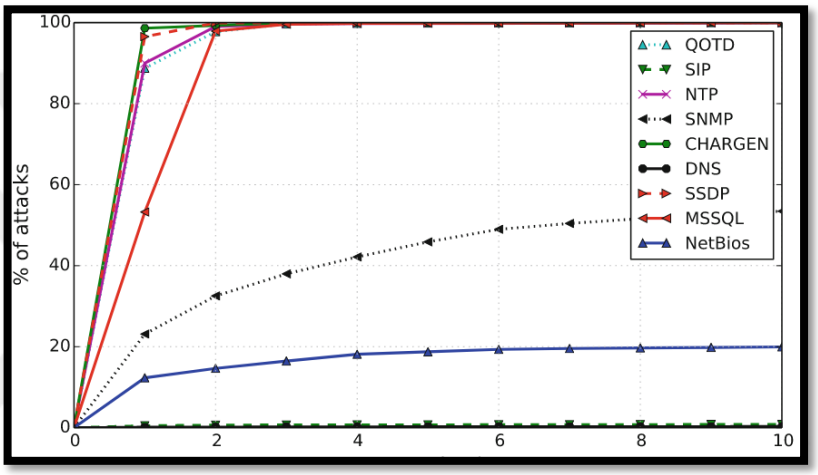
Şekil 5.1: Kullanılan Topoloji.

5.2. Veri Seti

AmpPot [33] veri seti, saldırı deneyleri için temel olarak kullanılmıştır. Bu veri seti bir honeypod üzerindeki DRDoS yakalama işleminden alınmıştır. AmpPot tarafından yakalanan trafik verilerini (PCAP) içerir. Bu veri seti, 31 Mayıs 2015 – 6 Ocak 2016 tarihleri arasında, AmpPot için PCAP dosyalarını içermektedir. Veriler yalnızca CharGen, DNS, NTP, SSDP sorgu paketlerini içermektedir. Booter [33], 2013 yılında yaklaşık 250 GB gerçek dünya DDoS trafiği içermektedir. Bu veri seti ise, önerilen sistemi test etmek ve normal DNS trafiği verilerini sağlamak için kullanılmıştır. İlgili çalışmadan alınan saldırı sayıları, Şekil 5.2'de gösterilmiştir. Şekil 5.3'de ise, saldırılar türleri için UDP yükleri gösterilmiştir.



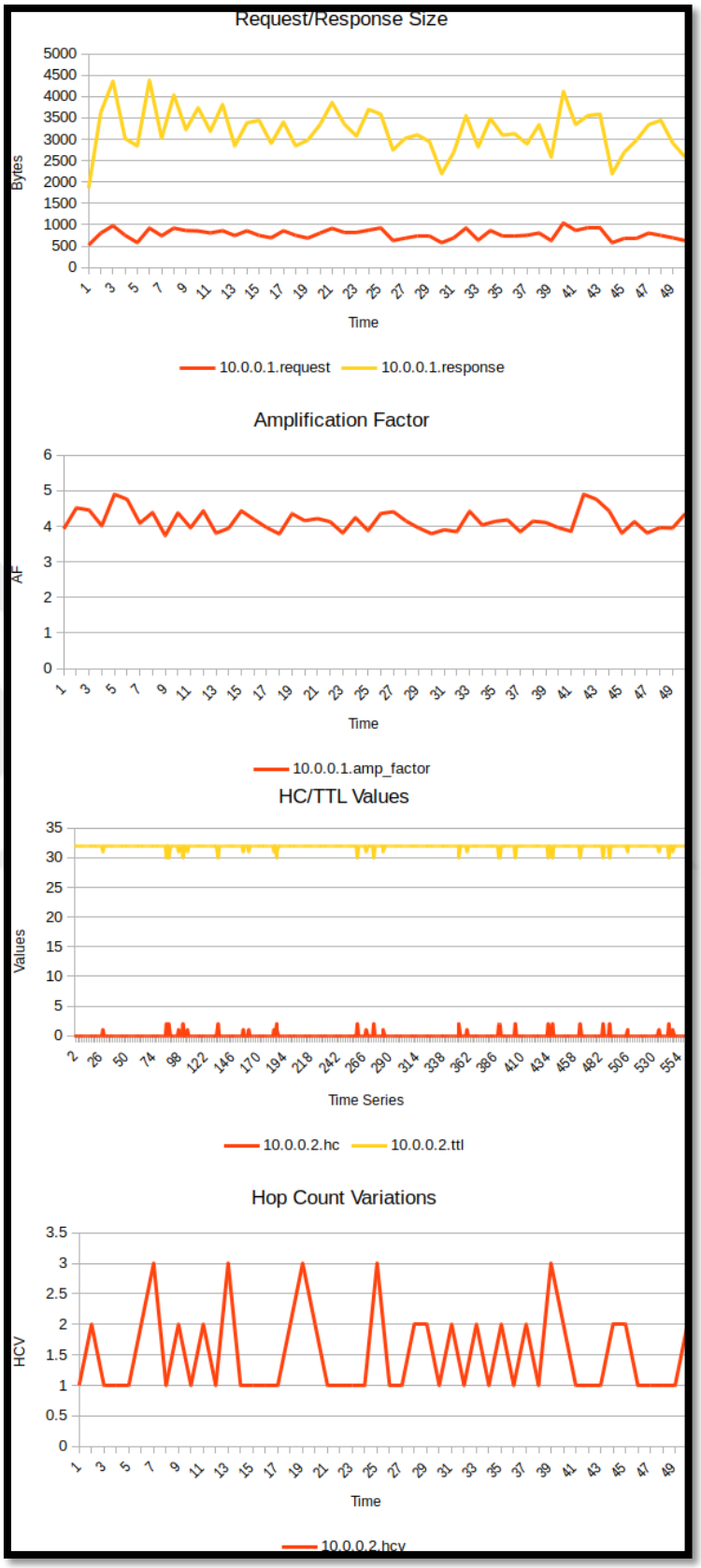
Şekil 5.2: Protokol ve gün bazında saldırı sayıları.



Şekil 5.3: Saldırı türlerinin UDP yükleri.

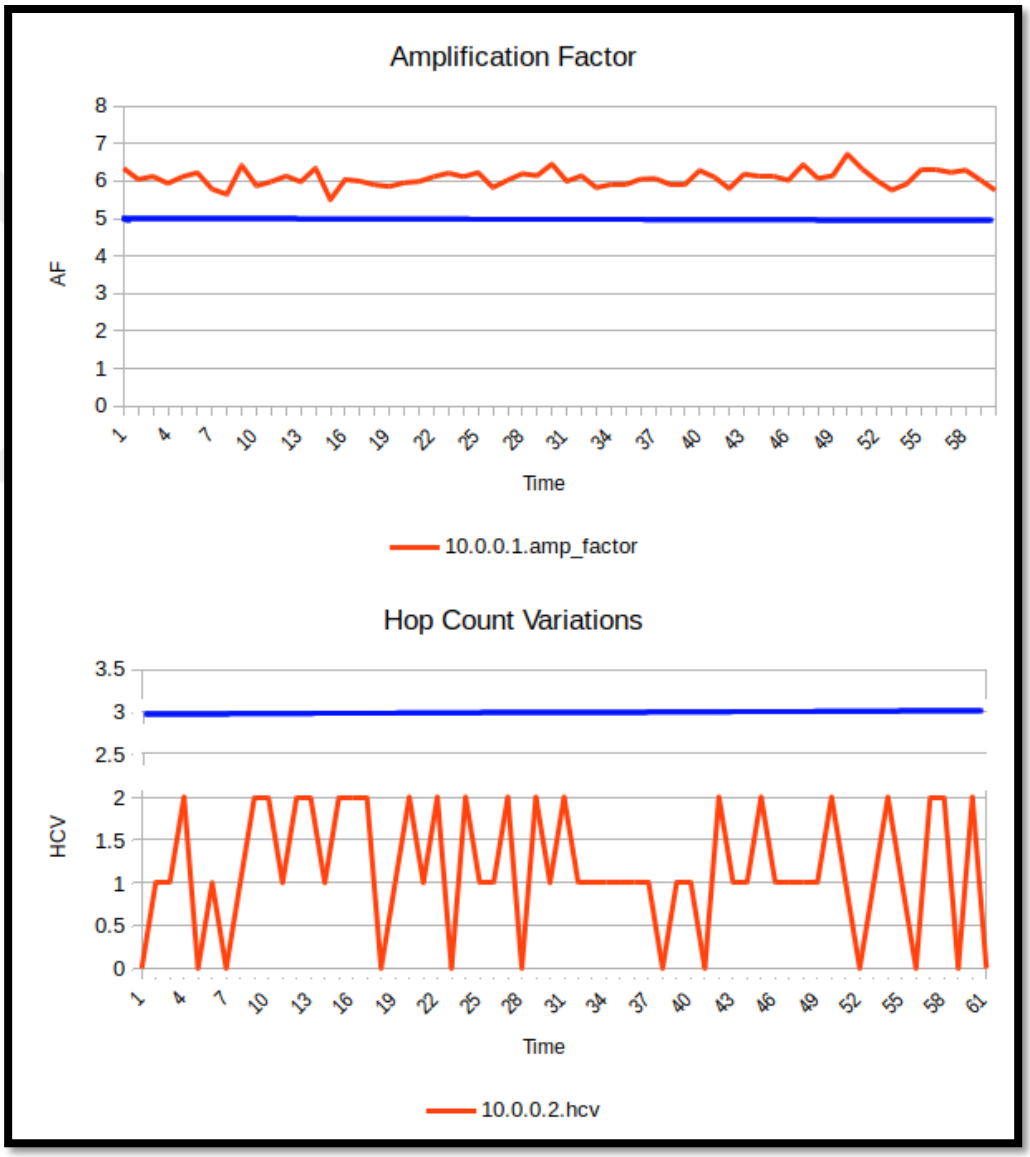
5.3. Deneyler

Booter [34], verileri, yukarıda belirtilen veri kümelerini kullanarak normal trafik akışları sağlamak için kullanılmıştır. Grafikleri baktığımızda Şekil 5.4 üzerinde düzenli bir istek/yanıt oranı ve HC/TTL değişimi görülmektedir. Bu grafikler, metrikler kullanılarak hesaplanan tüm AF ve HCV değerleridir. Bundan sonra sadece AF ve HCV grafiklerine bakmamız yeterli olacaktır. Sırasıyla normal trafik akışı, TXT kaydı denemeleri, DNS kuvvetlendirme saldırısı ve engellenmesi ve benzer saldırının NTP için denenmesi yapılacaktır. Bu deneyler sayesinde, YARASA için tespit, engelleme/azaltma kabiliyetleri gözlemlenebilecektir. Özellikle kullanılan veri setinin gerçek bir saldırıdan alınıyor olması, YARASA kabiliyetlerinin ölçülmesini daha önemli hale getirmektedir.



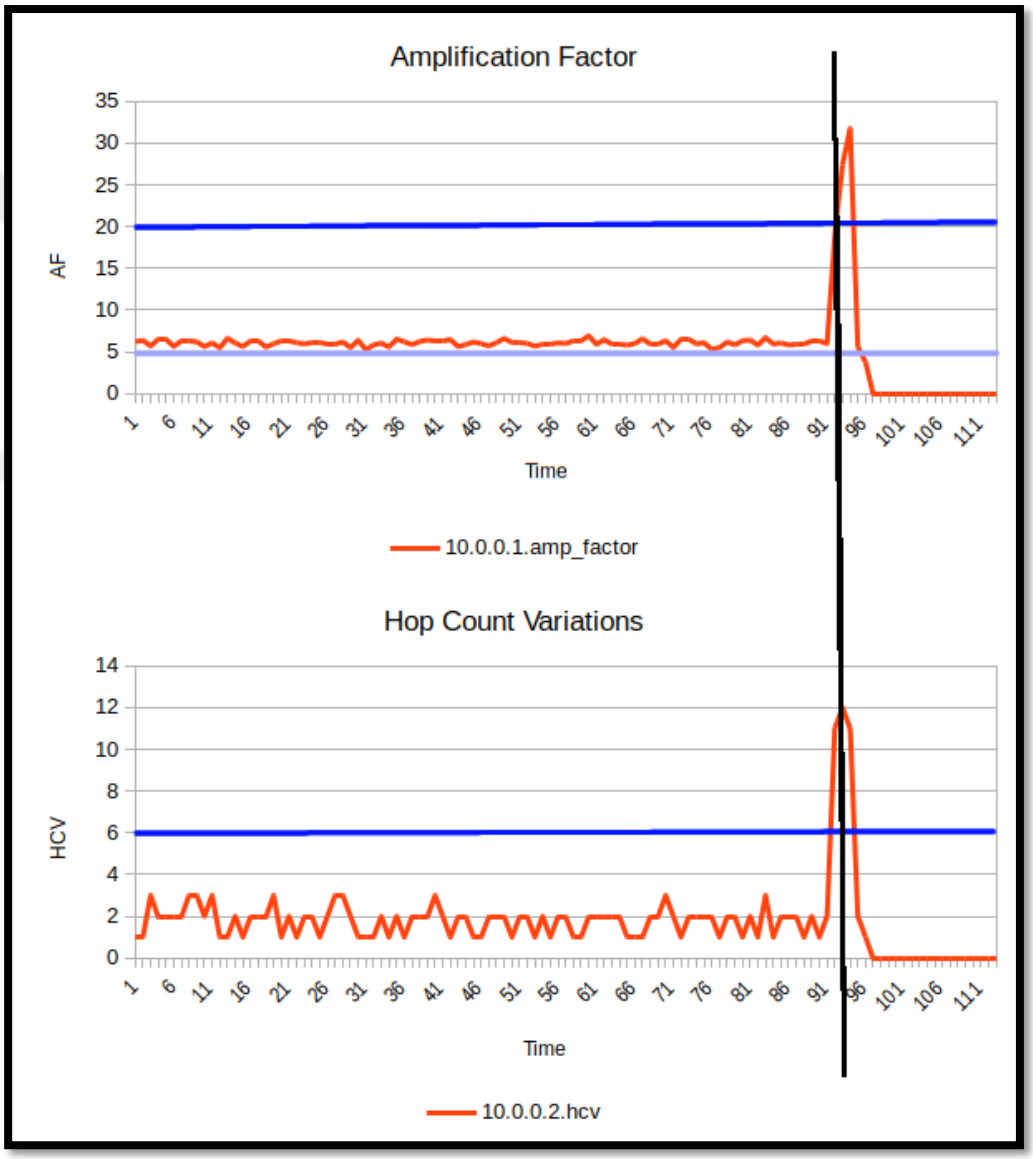
Şekil 5.4: Normal trafik metrikleri.

Yüksek trafikli bir TXT sorgusu olan bir trafik oluşturduğumuzda ve AF eşiğini 5 HCV eşiğini de 3 olarak ayarladığımızda, Şekil 5.5 ‘deki değerleri görüyoruz. Eşikte olmasına rağmen AF eşiği birkaç kez aşıldı. Ancak, herhangi bir engelleme mekanizması gözlemlenmedi. Çünkü bir saldırı olduğunda HCV değerinin değişmesini bekliyoruz. Bu yüzden sadece AF değerine bakan bir sistem tercih edilmemiştir. Bu sistemin önemi bu gibi ara değerlerde ortaya çıktığından, belirli bir AF değerine bakmaya gerek yoktur. Örneğin: DNS altyapısı yüksek AF değerleri üretebilir. Ancak bu bir saldırı olduğu anlamına gelmemektedir.



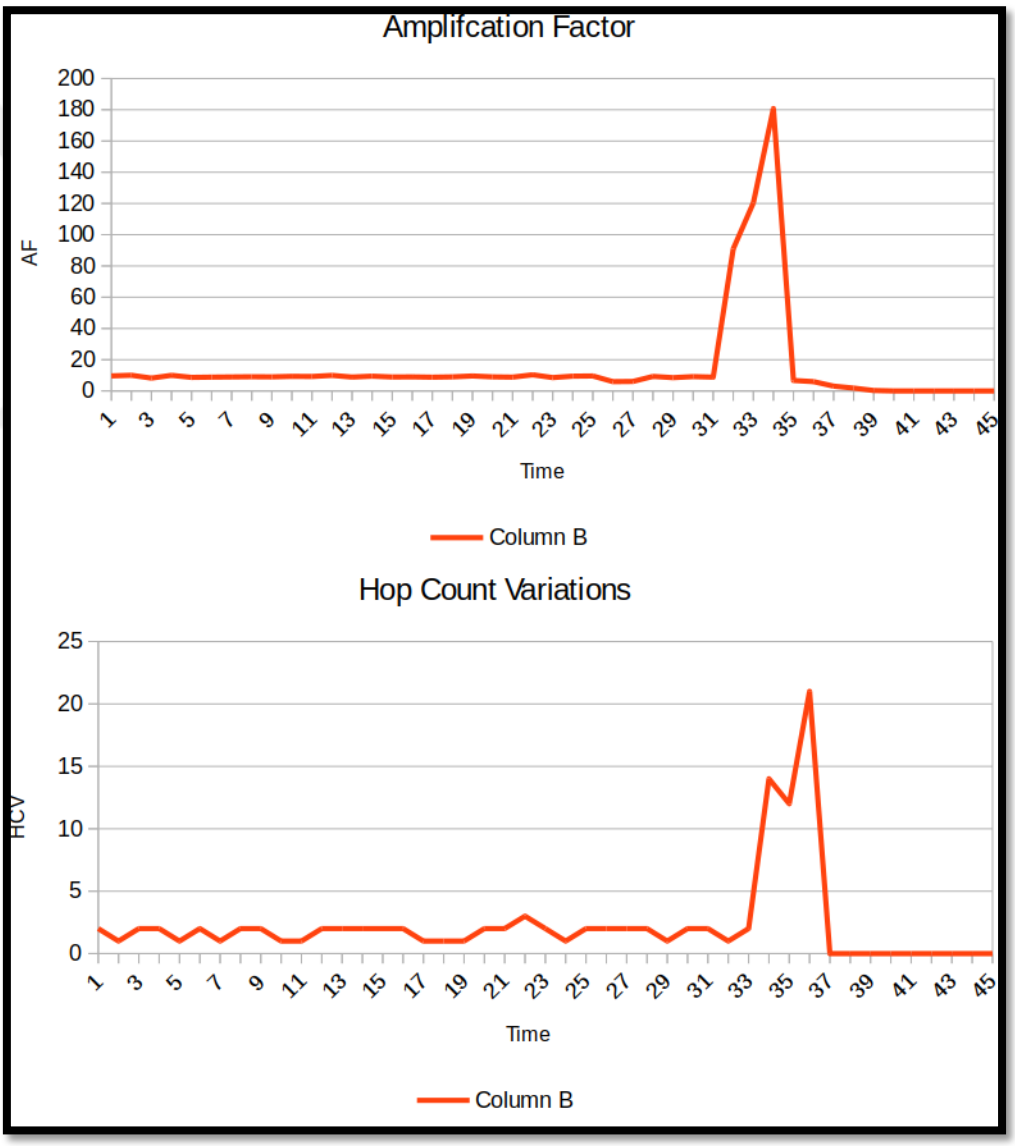
Şekil 5.5: Yoğun istekli TXT sorguları, AF ve HCV değerleri.

Faz 1 eşik değerinin 5 olduğunu varsayalım, bu trafik önleme aşamasına hiçbir zaman girmez. Faz 1 eşiğinin 5, faz 2 eşiğinin 20 ve HCV eşiğinin değerinin 6 olduğunun varsayalım. Şekil 5.6'da görülebilecek olan saldırıya bir göz atalım. Aslında 10 dakikalık bir grafik olmasına rağmen saldırıyı engelleme anı 1 dakikalık bir pencerede görülebilir. AF 'deki anlık yükselme sayesinde direk aşama 2'ye geçildi ve Open Resolver DNS sunucularındaki yanıt trafiği anında düştü, çünkü HCV eşik değerden daha yüksektir. Burada SDN ve yüksek ayarlanabilirlik sağlayan merkezi yapı, tespit edilen saldırılara karşı derhal harekete geçmemizi mümkün kılmıştır.



Şekil 5.6: DNS kuvvetlendirmeli saldırı, AF ve HCV değerleri.

Buradaki etki azaltma hızının asıl nedeni, bir saldırının sistemde tanımlandığından daha yüksek olan aşama 2 eşik değerinin üzerinde gerçekleşmesidir. Böylece, HCV değeri hesaplanmasına gerek kalmadan doğrudan azaltma aşamasına geçmek mümkündür. HCV değeri tüm istemciler için hesaplanmakta ve oldukça fazla kaynak tüketmektedir. UDP tabanlı kuvvetlendirme saldırılarının karakteristiği benzer olduğundan sahip olduğumuz veri setinde NTP saldırısı da test edilmiştir (Şekil 5.7). Benzer şekilde, saldırıyı hafifletme başarılı olmuştur. Bu, önerilen sistem için doğru eşiklerin belirlenebilmesi durumunda, birçok UDP tabanlı DRDoS saldırılarının önlenebilmesi anlamına gelmektedir.



Şekil 5.7: NTP kuvvetlendirmeli saldırı, AF ve HCV değerleri.

6. SONUÇLAR VE ÖNERİLER

Sonuç olarak, önerilen sistem gerçek veri setlerinde test edilmiş ve SDN üzerinde hızlı bir tespit ve engelleme gerçekleştirdiği tespit edilmiştir. Sistem DNS protokolüne özgü bir inceleme yapmadığından, UDP tabanlı DRDoS saldırılarının tespiti ve engellenmesi için uygun bulunmuştur. Sistem her DNS sunucusu ve istemcisi için bir tablo tutmamaktadır. Sadece basit bir TTL değişimi/entropisi hesaplamaktadır. Böylece daha az kaynak harcayarak bu saldırıları önleyebilmektedir. İki aşamalı yapısı ile kaynakları sadece ihtiyaç olduğu zaman harcamaktadır. Ayrıca SDN denetleyicisinde, YARASA sadece 4. katmana kadar paketleri çözmekte ve uygulama katmanına çıkmayarak daha hızlı bir tespit mekanizması sunmaktadır. Özetle YARASA, UDP tabanlı kuvvetlendirme/yansıma saldırılarını duyarlı bir biçimde engelleyen, uyarlanabilir ve hafif bir sistem olarak gerçeklenmiştir. Literatürde görüleceği gibi [12] [18], ML tabanlı sistemler oldukça fazladır. Bir ML temelli tespit şeması gelecekte tespit fazı için tahmin sistemi gerçeklenebilir. Bu çalışmada gerçekleştirilen tüm deneyler IPv4 protokolü için yapılmıştır. IPv6'ya özgü bir çalışma henüz yapılmamıştır. Duyarlı yapısı önceden bilgi sahibi olmadan çalışmasını sağlamaktadır. Daha aktif bir yapı ve hız sınırlama özellikleri gelecekte gerçeklenebilir. TTL değişimini hesaplamak için daha iyi bir fonksiyon geliştirilebilir. Şu andaki sistem belli bir penceredeki değişik TTL değerlerini almaktadır. Oysaki değişiklik ve iki TTL arasındaki farkı içeren başka bir alan formülü üzerine düşünülebilir. Bir gelecek işi olarak, hali hazırda var olan açık kaynak bir IDS üzerine entegre edilebilir. Daha büyük ve dağıtık veri setleri üzerinde de deneyler yapılabilir. Ayrıca HCV için daha iyi bir istatistiksel metot hesaplanabilir. Son olarak ise, önerilen yöntem hali hazırda kullanılan bir araç için gerçeklenebilir.

KAYNAKLAR

[1] Scott-Hayward, S., Natarajan S., Sezer S., (2015), "A survey of security in software defined networks", IEEE Communications Surveys & Tutorials, 18 (1), 623-654.

[2] Ahmad I., Namal S., Ylianttila M., Gurtov A., (2015), "Security in Software Defined Networks: A Survey", IEEE Communications Surveys & Tutorials, 17 (4), 2317-2346.

[3] Kreutz D., Ramos F., Verissimo, P., (2013), "Towards secure and dependable software-defined networks", Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking, 55-60, Hong Kong, China, 12-16 August.

[4] Web 1, (2019), https://techblog.comsoc.org/2019/01/28/ihs-markit-sdn-deployed-by-78-of-global-service-providers-at-end-of-2018/, (Erişim Tarihi: 12/8/2019).

[5] Akhunzada A., Ahmed E., Gani A., Khan M. K. Imran, M., Guizani S., (2015), "Securing software defined networks: taxonomy, requirements, and open issues", IEEE Communications Magazine, 53 (4), 36-44.

[6] Ryba F. J., Orlinski M., Wählisch M., Rossow C., Schmidt T. C., (2015), "Amplification and DRDoS attack defense--a survey and new perspectives", Technical Report No: arXiv-1505.07892, Open Archive: arXiv.org.

[7] Rudman L., Irwin B., (2015), "Characterization and analysis of NTP amplification based DDoS attacks" Information Security for South Africa (ISSA), 1-5, Johannesburg, South Africa, 12-13 August.

[8] Web 2, (2013), https://www.fiercetelecom.com/telecom/spamhaus-ddos-was-just-a-warning-shot, (Erişim Tarihi: 12/08/2019).

[9] Web 3, (2019), http://openresolverproject.org/, (Erişim Tarihi: 12/08/2019).

[10] Web 4, (2019), https://www.techrepublic.com/article/dns-amplification-attacks-increase-by-1000-since-2018/, (Erişim Tarihi: 12/08/2019).

[11] Web 5, (2018), https://blog.cloudflare.com/memcrashed-major-amplification-attacks-from-port-11211/, (Erişim Tarihi: 11/08/2018).

[12] Dharma N. G., Muthohar M. F., Prayuda J. A., Priagung K., Choi, D., (2015), "Time-based DDoS detection and mitigation for SDN controller", 17th Asia-Pacific Network Operations and Management Symposium (APNOMS), 550-553, Busan, South Korea, 19-21 August.

[13] Kalkan K., Altay L., Gür G., Alagöz, F., (2018), "JESS: Joint Entropy-Based DDoS Defense Scheme in SDN", IEEE Journal on Selected Areas in Communications, 36 (10), 2358-2372.

[14] Kalkan K., Gür G., Alagöz F., (2017), "SDNScore: A statistical defense mechanism against DDoS attacks in SDN environment", IEEE Symposium on Computers and Communications (ISCC), 669-675, Heraklion, Greece, 3-6 July.

[15] Wang R., Jia Z., Ju, L., (2015), "An entropy-based distributed DDoS detection mechanism in software-defined networking", IEEE Trustcom/BigDataSE/ISPA, 310-317, Helsinki, Finland, 20-22 August.

[16] Li L., Zhou J., Xiao N., (2007), "DDoS attack detection algorithms based on entropy computing", International Conference on Information and Communications Security, 452-466, Heidelberg, Germany, 12-15 December.

[17] Kumar K., Joshi R. C., Singh K., (2007), "A distributed approach using entropy to detect DDoS attacks in ISP domain", International Conference on Signal Processing, Communications and Networking, 331-337, Chennai, India, 22-24 February.

[18] Jin C., Wang H., Shin K. G., (2003), "Hop-count filtering: an effective defense against spoofed DDoS traffic", 10th ACM conference on Computer and communications security, 30-41, New York, USA, 3 October.

[19] Chen C. C., Chen Y. R., Lu W. C., Tsai S. C., Yang M. C. (2017), "Detecting amplification attacks with software defined networking", IEEE conference on dependable and secure computing, 195-201, Taipei, Taiwan, 7-10 August.

[20] Aizuddin A. A., Atan M., Norulazmi M., Noor M. M., Akimi S., Abidin Z. (2017), "DNS amplification attack detection and mitigation via sFlow with security-centric SDN", 11th International Conference on Ubiquitous Information Management and Communication, 1-7, At Beppu, Japan, 5-7 January.

[21] Huistra D., (2013), "Detecting reflection attacks in DNS flows", 19th Twente Student Conference on IT, Enschede, Netherlands, 1 January.

[22] Zheng J., Li Q., Gu G., Cao J., Yau D. K., Wu J., (2018), "Realtime DDoS defense using COTS SDN switches via adaptive correlation analysis", IEEE Transactions on Information Forensics and Security, 13 (7), 1838-1853.

[23] Kambourakis G., Moschos T., Geneiatakis D., Gritzalis S., (2007), "A fair solution to dns amplification attacks", Second International Workshop on Digital Forensics and Incident Analysis (WDFIA), 38-47, Samos, Greece, 27-28 August.

[24] Yao G., Bi J., Xiao P., (2011), "Source address validation solution with OpenFlow/NOX architecture", 19Th IEEE international conference on network protocols, 7-12, Vancouver, BC, Canada, 17-20 October.

[25] Fayaz S. K., Tobioka Y., Sekar V., Bailey, M., (2015), "Bohatei: Flexible and elastic ddos defense", 24th USENIX Security Symposium, 817-832, Washington, USA, 12-14 August.

[26] Rossow C., (2014), "Amplification Hell: Revisiting Network Protocols for DDoS Abuse", Network and Distributed System Security Symposium, 23-26 February.

[27] Anagnostopoulos M., Kambourakis G., Gritzalis S., Yau D. K., (2018), "Never say never: Authoritative TLD nameserver-powered DNS amplification", IEEE/IFIP Network Operations and Management Symposium, 1-9, Taipei, Taiwan, 23-27 April.

[28] Fachkha C., Bou-Harb E., Debbabi M., (2014), "Fingerprinting internet DNS amplification DDoS activities", 6th International Conference on New Technologies, Mobility and Security (NTMS), 1-5, Dubai, United Arab Emirates, 30 March-2 April.

[29] van Rijswijk D. R., Sperotto A., Pras, A., (2014), "DNSSEC and its potential for DDoS attacks: a comprehensive measurement study", Conference on Internet Measurement Conference, 449-460, Vancouver, BC, Canada, 5-7 November.

[30] Yamada R., Goto S., (2013), "Using abnormal TTL values to detect malicious IP packets", Asia-Pacific Advanced Network, 27-34, Nallur Kandaswamy Temple, Nallur, Sri Lanka Cover Page, 20 May.

[31] Scheitle Q., Gasser O., Emmerich P., Carle G., (2016), "Carrier-Grade Anomaly Detection Using Time-to-Live Header Information", Technical Report No: arXiv:1606.07613, Open Archive: arXiv.org.

[32] Web 5, (2013), https://www.us-cert.gov/ncas/alerts/TA13-088A, (Erişim Tarihi: 12/08/2019).

[33] Krämer L., Krupp J., Makita D., Nishizoe T., Koide T., Yoshioka K., Rossow C., (2015), "Amppot: Monitoring and defending against amplification ddos attacks", Lecture Notes in Computer Science, vol 9404, Springer.

[34] Santanna J. J., van Rijswijk-Deij R., Hofstede R., Sperotto A., Wierbosch M., Granville L. Z., Pras, A., (2015), "Booters - An analysis of DDoS-as-a-service attacks", IFIP/IEEE International Symposium on Integrated Network Management (IM), 243-251, Ottawa, ON, Canada, 11-15 May.

ÖZGEÇMİŞ

Kaan ÖZDİNÇER 1988 yılında İstanbul'da doğdu. 2010 yılında Çanakkale Onsekiz Mart Üniversitesi, Bilgisayar Mühendisliği bölümünden mezun oldu. 2010 yılında Çanakkale Onsekiz Mart Universitesi bünyesinde "Ulusal IPv6 Altyapısı Tasarımı ve Geçişi Projesi", 2011-2012 yıllarında TUBİTAK UEKAE "Pardus Projesi" nde araştırmacı ve Linux Sistem Yöneticisi olarak çalıştı. 2012 yılında Gebze Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalında yüksek lisans eğitimine başladı. 2012 yılından bu yana, özel şirketlerde Linux Sistem Yöneticisi olarak çalışmaya devam etmektedir.

EKLER

Ek A: Tez Çalışması Kapsamında Yapılan Yayınlar

Özdinçer, K., Mantar, H. A., (2019), "SDN-based Detection and Mitigation System for DNS Amplification Attacks", 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), 1-7, Ankara, Turkey, 11-13 October.