T.C. İSTANBUL TİCARET ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

DDOS SALDIRILARININ TESPİT EDİLMESİNDE MAKİNE ÖĞRENİMİ YÖNTEMLERİNİN UYGULANMASI

Tuğba AYTAÇ

Danışman
Prof. Dr. Abdül Halim ZAİM

Eş Danışman
Doc. Dr. Muhammed Ali AYDIN

YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
İSTANBUL - 2020

KABUL VE ONAY SAYFASI

Tuğba AYTAÇ tarafından hazırlanan "**DDOS Saldırılarının Tespit Edilmesinde Makine Öğrenimi Yöntemlerinin Uygulanması"** adlı tez çalışması 08/09/2020 tarihinde aşağıdaki jüri üyeleri önünde başarı ile savunularak, İstanbul Ticaret Üniversitesi Fen Bilimleri Enstitüsü **Bilgisayar Mühendisliği Anabilim Dalı**'nda **Yüksek Lisans Tezi** olarak kabul edilmiştir.

Danışman	**Prof. Dr. Abdül Halim ZAİM** İstanbul Ticaret Üniversitesi	.....
Jüri Üyesi	**Dr. Öğr. Üyesi Mustafa Cem KASAPBAŞI** İstanbul Ticaret Üniversitesi	.....
Jüri Üyesi	**Dr. Öğr. Üyesi Zeynep TURGUT** Haliç Üniversitesi	.....

Onay Tarihi : 18/09/2020

İstanbul Ticaret Üniversitesi, Fen Bilimleri Enstitüsünün 18.09.2020 tarih ve 2020/290 numaralı Yönetim Kurulu Kararının 2. maddesi gereğince, ders yüklerini ve tez yükümlülüğünü yerine getirdiği belirlenen "Tuğba AYTAÇ" (TC:17233561536) adlı öğrencinin mezun olmasına oy birliği ile karar verilmiştir.

Prof. Dr. Necip ŞİMŞEK
Enstitü Müdürü

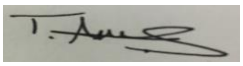
AKADEMİK VE ETİK KURALLARA UYGUNLUK BEYANI

İstanbul Ticaret Üniversitesi, Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında,

- tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu,
- başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
- atıfta bulunduğum eserlerin tümünü kaynak olarak gösterdiğimi,
- kullanılan verilerde herhangi bir tahrifat yapmadığımı,
- ve bu tezin herhangi bir bölümünü bu üniversitede veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı

beyan ederim.

18/09/2020



Tuğba AYTAÇ

İÇİNDEKİLER

Sayfa

ÖZET

Yüksek Lisans Tezi

DDOS SALDIRILARININ TESPİT EDİLMESİNDE MAKİNE ÖĞRENİMİ YÖNTEMLERİNİN UYGULANMASI

Tuğba AYTAÇ

İstanbul Ticaret Üniversitesi
Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı

Danışman: Prof. Dr. Abdül Halim ZAİM

Eş Danışman: Doc. Dr. Muhammed Ali AYDIN
2020, 67 sayfa

İnternet ihtiyacının ve kullanıcı sayısının artmasıyla siber güvenlik kavramının önemi ortaya çıkmıştır. Günümüzde kullanılan saldırı tespit sistemlerinden imza tabanlı saldırı tespit sistemleri daha önce yapılmış saldırıları belleğinde tutarak meydana gelebilecek saldırıları tespit ederken, anomali tabanlı saldırı tespit sistemleri daha önce karşılaşılmamış saldırılara ilişkin çıkarımlar yapabilmektedir.

Bu çalışmanın amacı saldırı tespit sistemlerinde farklı metotlar kullanılarak saldırı tespitindeki başarı oranlarını analiz etmektir. Çalışmada CICDDoS2019 veri seti kullanılmış olup söz konusu veri setinde bulunan DDOS saldırılarının, makine öğrenme metotlarından; Yapay Sinir Ağları (YSA), Destek Vektor Makinesi (DVM), Gaussian Naive Bayes, Multinomial Naive Bayes, Bernoulli Naive Bayes, Logistic Regresyon, K-nearest neighbour (KNN), Decision Tree (entropy-gini) ve Random Forest algoritmaları kullanılarak tehdidin tespitindeki başarı oranları analiz edilerek karşılaştırılmıştır. Başarı oranlarında en yüksek oranın K-nearest neighbor, Logistic Regrasyon, Naive Bayes, (Multinomial - Bernoulli) algoritmaları kullanılarak gerçekleştirilen, % 100'e yakın başarı sağlayan modeller olduğu görülmüştür.

Anahtar Kelimeler: CICDDoS2019, DDOS, makine öğrenme metotları, saldırı tespit sistemleri.

ABSTRACT

M.Sc. Thesis

APPLICATION OF MACHINE LEARNING METHODS IN DETERMINING DDOS ATTACKS

Tuğba AYTAÇ

İstanbul Commerce University
Graduate School of Applied and Natural Sciences
Department of Computer Engineering

Supervisor: Prof. Dr. Abdül Halim ZAİM

Co-Supervisor: Assoc. Prof. Dr. Muhammed Ali AYDIN

2020, 67 pages

The increasing demand for communication since the existence of humanity has gained momentum as the internet concept has entered our daily lives. The importance of cyber security has become evident with the increasing need of the Internet and the number of users. While signature-based intrusion detection systems detect the attacks that may occur by keeping previous attacks in memory, anomaly-based intrusion detection systems can make inferences about unexpected attacks.

The aim of this study is to analyze the success rates of intrusion detection by using different methods in intrusion detection systems. CICDDoS2019 data set was used in the study, and DDOS attacks in the said data set are among the machine learning methods; Artificial Neural Networks (ANN), Support Vector Machine (DVM), Gaussian Naive Bayes, Multinomial Naive Bayes, Bernoulli Naive Bayes, Logistic Regression, K-nearest neighbor (KNN), Decision Tree (entropy-gini) and Random Forest algorithms The success rates in the determination were analyzed and compared. It has been observed that the highest rate of success rates are the models, which are realized by using K-nearest neighbor, Logistic Regression, Naive Bayes, (Multinomial - Bernoulli) algorithms, and provide nearly 100% success.

Keywords: CICDDoS2019, DDOS, intrusion detection system, machine learning methods.

TEŞEKKÜR

Tez çalışmam sırasında gösterdiği her türlü ilgi, destek ve anlayış için değerli danışman hocam Prof. Dr. Abdül Halim ZAİM'e ve eş danışman hocam sayın Doc. Dr. Muhammed Ali AYDIN 'a, bilgi, birikim ve tecrübeleriyle her zaman desteklerini esirgemeyen ve çalışma yaşamımda kendime örnek edindiğim yöneticim Dilek METE HANGÜL'e ve bu süreçte destek olan değerli çalışma arkadaşlarıma, her anımda yanımda olan, aldığım her kararda beni yanlız bırakmayan ve yardımlarını esirgemeyen aileme sonsuz teşekkürlerimi sunarım.

Tuğba AYTAÇ
İSTANBUL, 2020

ŞEKİLLER

Sayfa

ÇİZELGELER

Sayfa

SİMGELER VE KISALTMALAR

ACK	Acknowledgement
ARP	Address Resolution Protocol
ARPANET	Advanced Research Projects Agency Network
CERIAS	Center for Education and Research Information Assurance and Security
CPU	Central Processing Unit
DDOS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DIDS	Distributed Intrusion Detection System
DNS	Domain Name System
DVM	Destek Vektor Makinesi
FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
ICMP	Internet Control Message Protocol
IDES	Intrusion Detection Expert System
IDIOT	Intrusion Detection In Our Time
IDS	Intrusion Detection Systems
IP	Internet Protocol
IPS	Intrusion Prevention System
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
KNN	K-nearest neighbour
MAC	Media Access Control
MIDAS	Multics Intrusion Detection and Alerting System
NADIR	Network Anomaly Detection and Intrusion Reporter
NCSC	Computer Science Laboratory
NSM	Network Security Monitor
POP	Post Office Protocol
R2L	Yönetici Hesabı ile Yerel Oturum Açma (Remote to Local)
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SRI	Stanford Araştırma Enstitüsü
STS	Saldırı Tespit Sistemi
SYN	Synchronize
TCP/IP	Transmission Control Protocol / Internet Protocol
TCP	Transmission Control Protocol
U2R	Kullanıcı Hesabının Yönetici Hesabına Yükseltilmesi (User to root)
UDP	User Datagram Protocol
VPN	Virtual Private Network
W&S	Wisdom and Sense–Hikmet ve His
YSA	Yapay Sinir Ağları

1. GİRİŞ

Gelişen teknoloji ile günlük hayatımızda vazgeçilmez bir unsur haline gelen internet bankacılık, sağlık gibi birçok sektörde ve sosyal hayatımızda oldukça geniş yer kaplamaktadır. 1969 yılında ortaya çıkan, çok az sayıda cihazın haberleşmesini sağlayan ve internetin temelini oluşturan ARPANET (Advanced Research Projects Agency Network) ile bir ağ sistemi olan internete 2020 yılına kadar yaklaşık olarak 50 milyar nesnenin bağlı olacağı öngörülmektedir (Evans, 2016). İnternetin ilk olarak e-posta ve dosya gönderiminde kullanılırken günümüzde birçok sistemin birbiriyle haberleştiği üzerinde büyük boyutlarda trafik akışının meydana geldiği devasa bir ağ halini almıştır.

Bilgisayar ağlarının yaygın olarak kullanımı ağa bağlı sistemlere yapılan saldırıların da artışına neden olmuştur. DDOS (Distributed Denial of Service – Dağıtık Hizmet Engelleme) saldırısı ise son zamanlarda bir çok kurumun maruz kaldığı saldırıların başında gelmektedir. Hedef sunucuyu ele geçirilen kurban bilgisayarlardan gelen oldukça yoğun bir trafiğe maruz bırakılarak verilen hizmetin engellenmesi sağlanmaktadır. Kurumsal veya günlük hayatımızda kullanılan ağları kötü niyetli kişilerden korumak için güvenlik duvarı, antivirus vb. birçok sistem veya yazılım kullanılmaktadır. Fakat söz konusu tedbirler saldırıların önününe geçmek için yetersiz kalabilmektedir. Çünkü karşımızda maddi kazanç veya itibar kaybetmemizi isteyen ve bir ekip halinde çalışan kişiler sistemlerdeki açıkları tespit edebilmek için sürekli olarak zafiyetleri bulmaya çalışmaktadır.

Güvenlik duvarı sistemine güvenmek kurumsal yada bireysel ağlara karşı yapılan saldırıların tespit edilerek engellenmesi yönünde tek başına yeterli değildir. Güvenlik duvarı sisteminin açıklarının kapatılmasında saldırı tespit sistemleri de kullanılmaktadır (Kaya ve Yıldız, 2014, s. 90).

Sistemlere karşı yapılacak olan saldırıların erken tespit edilmesi ve önlenmesi son derece önemlidir. Saldırı Tespit Sistemleri (STS), ağ üzerinden yapılan saldırılara karşı bilgi sistemlerinin korunmasında “alarm” niteliği taşıyan

yazılım ve/veya donanım bileşenleridir. STS'leri sistemlere yapılan yetkisiz erişimler ve kötüye kullanımları tespit ederek, saldırganların sistemlere sızma girişimleri engellenebilmektedir (Sağıroğlu vd., 2011) .

Bir STS tasarımında iki ana yaklaşım vardır (Zulkernine, 2004). Bu iki yaklaşım; her davranışa özel karakteri ile tespit eden İmza Tanıma Temelli saldırı tespiti ve ağ üzerinde oluşan anormal (abnormal) ağ trafiğinin incelenmesi ile saldırıları tespit eden sistemlerdir. Her iki yaklaşımın öncelikli amacı saldırıların tespitinin gerçek zamana yakın olarak yapılabilmesi ve saldırının neden olduğu hasarın giderilmesi veya en aza indirilmesi için belli başlı saldırıları karantina altına alabilmektir (Ratinder ve Maninder, 2014).

Bu çalışmanın amacı DOS ataklarının makine öğrenme metotlarıyla mümkün olan en kısa sürede yüksek başarı oranında tespit eden sistemi tasarlamaktır. Çalışmada veri seti Anomali Tabanlı Saldırı Tespit Sistemlerinden olan makine öğrenme metotları kullanılmış ve oluşturulan veri setlerinde eğitim gerçekleştirilmiştir. 4'lü, 6'lı ,8'li, 10'lu ve 12'li özelliğe sahip veri setleri oluşturularak en yüksek başarı oranıyla en hızlı tespiti gerçekleştiren değerlerin bulunması hedeflenmiştir. Öznitelik değerlerinin az sayıda tutularak saldırının tespit edilmesi STS'nin performansı açısından önemlidir.

1.1 Tezin Amacı

Tez kapsamında CICDDoS2019 güncel veri seti kullanılarak DDOS saldırılarına ait en iyi özellikler farklı metotlar kullanılarak tespit edilmeye çalışılmıştır. Makine öğrenme metotlarından; Yapay Sinir Ağları (YSA), Destek Vektor Makinesi (DVM), Gaussian Naive Bayes, Multinomial Naive Bayes, Bernoulli Naive Bayes, Logistic Regresyon, K-nearest neighbour (KNN), Decision Tree (entropy-gini) ve Random Forest algoritmaları kullanılarak tehdidin tespit edilmesindeki başarı oranları analiz edilerek tehdidin en kısa sürede ve yüksek başarı oranında tespiti amaçlanmıştır.

1.2 Tezin Organizasyonu ve Katkıları

Tez çalışmasının birinci bölümünde, tezin genel olarak içeriğinin neler olduğuna ve bu konuda çalışma amacına yönelik temel bilgilere yer verilmiştir. Diğer bölümlere ilişkin açıklamalar aşağıda yer almaktadır.

Bölüm 2'de, ağ güvenliğinin önemi vurgulanmış, sistemlere yönelik yapılan saldırıların maruz kalabileceği protokollere yönelik detaylı açıklamalara yer verilmiştir.

Bölüm 3'te, kurum ve sistemlere yönelik gerçekleştirilebilecek saldırılar, söz konusu saldırılar için yararlanılan zafiyetler ve alınması gereken önlemler vurgulanmıştır.

Bölüm 4'te, STS'lerin tarihçesi, kullanılmasındaki avantajlar, mimari yapısı ve mevcut saldırı tespit sistemlerinin özelliklerine detaylı bir şekilde yer verilmiştir.

Bölüm 5'te, DDOS atakların tespit edilmesine yönelik tez çalışmamda makine öğrenimi metotlarını kullanarak CICDDoS2019 veri kullanılarak saldırı tespitindeki başarı oranlarının analizi gösterilmiştir.

Bölüm 6'da, farklı algoritmalar ile eğitimi gerçekleştirilen veri içerisinden en yüksek doğruluk oranı sonuçlarını veren algoritmalara ve saldırının tespit edilmesinde belirleyici en iyi özelliklerin neler olduğu ifade edilmiştir.

2. LİTERATÜR ÖZETİ

2.1. Ağ Güvenliği ve Protokoller

Protokoller, birbirine bağlı sistemlerin haberleşmesi için önemli rol oynamaktadır. Protokollerin içerisinde iletilecek veri, hedef adres, iletimin sağlanacağı yol gibi birçok bilgi barındırmaktadır. Sistemlerin birbirleriyle haberleşmesi sağlanırken meydana gelebilecek saldırıların önlenmesi ağ güvenliğine yönelik gerekli tedbirlerin alınmasıyla mümkündür.

2.1.1. Ağ güvenliği ve önemi

Kurumlarda veya bireysel olarak kullanılan ağların internete bağlı olması dışarıdan gelebilecek tehlikelere karşı gereken önlemlerin alınması gerektirmektedir. Kurumun çalışanlarına gerektiği ölçüde sistemlere erişim izni vermesi ve ağ yapısında VPN (Virtual Private Network – Sanal Özel Ağ), Firewall, IDS (Intrusion Detection Systems – Saldırı Tespit Sistemi), IPS (Intrusion Prevention System – Saldırı Önleme Sistemi) gibi sistemlerle kurum ağının denetlenebilir hale getirilerek korunması sağlanabilmektedir (Fırlar, 2003, s. 12).

Ağ güvenliğinin sağlanması temel bilgi güvenliği prensiplerinin sağlanması ile mümkün olabilmektedir. Bütünlük, erişilebilirlik, gizlilik ve inkar edilememe özelliklerini barındıran yapı güvenilir bir yapıdır.

Bütünlük: Verinin değiştirilmesi, silinmesi veya yeni veri eklenmesinin engellenerek varolan verinin korunmasını sağlamaktır.

Gizlilik:Verinin yetkisiz kişiler tarafından ele geçirilmesinin önlenmesidir.

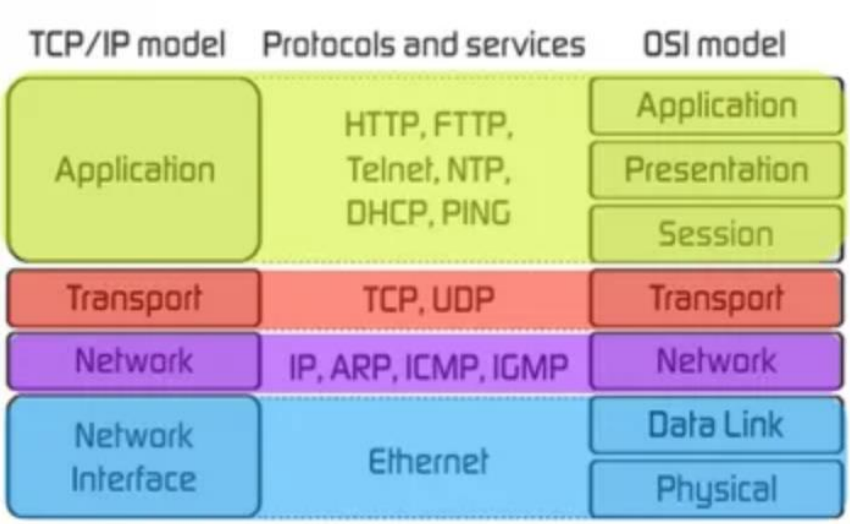
Erişilebilirlik: Yetkili kişiler tarafından gereken süre boyunca bilginin erişebilir olmasıdır.

İnkar edilememe: Veride değişiklik yapılması, verinin gönderilmesi veya alınması gibi işlemlerde kimin tarafından yapıldığının tespit edilebilmesidir.

2.1.2. Ağ protokolleri ve saldırı çeşitleri

Ağ protokolleri bilgisayar ve sistemlerin birbirleri arasındaki haberleşmenin nasıl yapılacağını belirleyen standartlardır. Veri içerisinde bulunan paketlerin yönlendirilmesi, sıralanması, hata kontrolleri söz konusu protokoller ile sağlanmaktadır.

İki bilgisayar arasındaki haberleşmenin katmanlar şeklinde yapıldığını tanımlayan OSI referans modeli fiziksel katman, veri bağı katmanı, ağ katmanı, taşıma katmanı, oturum katmanı, sunum ve uygulama katmanlarından oluşmaktadır. Ağ protokolleri ise ağ katmanında işlev görmektedir. OSI modelinden önce geliştirilen TCP/IP modeli teknolojinin gelişmesi ve artan güvenlik ihtiyacı ile yerini OSI modeline bırakmış durumdadır.



Şekil 2.1 TCP/IP ve OSI referans modeline ilişkin katmanlar

2.1.2.1. IPv4 (Internet Protocol Version 4)

İnternet Protokolü (IP) TCP/IP protokolleri arasında yer alan adresleme protokolüdür. Veri iletiminin adreslenerek paketler halinde iletilmesini

sağlayan protokoldür. Adresler 32bit uzunluğunda ve 8'er bitlik oktetlerden meydana gelmektedir. Veri paketleri başlık ve veri kısmından oluşmaktadır. Başlık kısmında, kaynak adresi, hedef adresi ve verinin iletimi için gerekli olan diğer bilgiler tutulur.

2.1.2.2. IPv6 (Internet Protocol Version 6)

IPv4'ün yetersiz kalmasıyla oluşturulan yeni nesil internet protokolüdür. IPv6 protokolüne geçilmesinde iki temel unsur yer almaktadır. IPv4'ün sunabildiği adres uzayının yetersiz kalması ve tasarımda bulunan açıkların giderilmesidir.

Tasarımın getirmiş olduğu açıkların SSL ve PGP ile giderilmeye çalışılsa da uçtan uca güvenli bir iletişim sağlayamamaktadır. IPv4'ün authentication mekanizmalarına yönelik eksikliği ortadaki adam saldırılarına, zayıf tasarımı ve dar adres alanı nedeniyle servis dışı bırakma ve özellikle portların hızlıca taranmasını sağlayan keşif tipi saldırılarılara maruz kalmasına yol açmaktadır (Pesen, 2020).

IPv4 ve IPv6 adresleme protokolleri arasındaki farklar Çizelge 2.1'de yer almaktadır (Pesen, 2020).

Çizelge 2.1 Pv4 ve IPv6 adresleme protokollerinin karşılaştırılması

	IPv4	IPv6
Güvenlik/Uzunluk	32 bit adres uzunluğu	128 bit adres uzunluğu
IPsec	Kullanımı seçeneğe bağlı	Uygulama desteği mecburidir
Quality of Service	IPv4 başlığında paket akışını tamamlamak için yönlendiricilerin kullanabileceği ortak bir stadrt QoS tanımlamaları yoktur	Başlıkta bulunan "flow label" alanı yönlendiriciler tarafından kullanılır

Fragmentation	Paketin parçalanması işlemi (fragmentation) hem ağdaki ara elemanlar hem de gönderici tarafından yapılabilir	Paketin parçalanması işlemi (fragmentation) yönlendiriciler tarafından yapılmaz. Sadece gönderen istemci tarafından yapılır
Checksum	Checksum vardır	Checksum içermez
Paket başlığında özel alanlar	Seçenekler alanı bulunur	Seçimli veriler extension headerlar ile taşınır
ARP	ARP kullanılır	ARP Request paketleri multicast Neighbor Solicitation mesajlarıyla değiştirilmiştir
Ağ geçidi tespiti	Varsayılan en iyi ağ geçidi tespiti için ICMP Router Discovery kullanılabilir, fakat zorunlu değildir	ICMP Router Discovery yerine "ICMPv6 Router Solicitation" ve "Router Advertisement" kullanılır ve kullanımı zorunludur
Broadcast	Ağdaki tüm birimlere "broadcast" adresleri ile erişilir	"broadcast" adresi bulunmamaktadır. Bunun yerine "link-locak scope all-nodes multicast" adresi kullanılır
Yapılandırma	DHCP server yardımıyla veya elle yapılandırılır	Otomatik olarak yapılandırılır

2.1.2.3. TCP (Transmission Control Protocol–İletim Kontrol Protokolü)

Taşıma katmanında yer alan TCP protokolü verinin hedef adrese ulaşıp ulaşmadığını kontrol etmektedir. Gönderi ve alıcı arasında uygulama katmanında oturum başlatıldıktan sonra iletimi sağlanacak olan veri paketlerini parçalara ayırarak sıra numarası vermektedir.

Bir alt katman olan ağ katmanına gelen veriye IP paketleri eklenir. IP protokolü ile gideceği hedef adres belirlenirken, TCP protokolü ile kullanacağı uygulama ve servis tarafından kullanacağı port numarası belirlenir.

TCP bağlantısının gerçekleştirilmesinden sonra hedef ve kaynak adresten emin olunması için istemci tarafından üçlü el şıkışma (Three Way Handshake) başlatılır.
Üç adımdan oluşturulan üçlü el sıkışma aşamaları aşağıda yer almaktadır (Başaranoğlu, 2020).

1. İstemcinin işletim sistemi tarafından rasgele belirlenen sıra numarası (Sequence Number) ile sunucuya SYN (Synchronize) biti / bayrağı 1 olan paket gönderilir. Sıea numarası sayesinde paketler alıcıya sıralı olarak gelmese bile alıcı taradınan söz konusu paketler sıralandırılmaktadır.

2. İkinci adım olarak istemci tarafından gönderilen paketi alan sunucu, istemciye göndereceği paketi hazırlar. SYN ve ACK (Acknowledgement) bayrakları 1 olarak ayarlanır. Ayrıca sıra numarasını bir arttırarak gönderilmek istenenen pakete ekler. Bu yolla sunucu istemciden gelen paketin doğru sırada olmasını ve bir sonraki kabul edeceği paketin sıra numarasını belirtmiş olmaktadır.

3. Son adım olarak ise istemci sunucunun gönderdiği paketi alarak bir sonraki paketi hazırlar. İstemciden sunucuya iletilen paketin ACK bayrağı 1 olarak ayarlanarak ACK numarası 642 olan paket gönderilmektedir.

2.1.2.4. UDP (User Datagram Protocol–Kullanıcı Veri Bloğu Protokolü)

UDP protokolü TCP/IP modelinin taşıma katmanında yer alan bir protokoldür. Bu protokol ile sağlanan veri aktarımında iletilen veri paketlerinin sıralı bir şekilde iletilip iletilmediği ve güvenilir olarak paketlerin sunucuya ulaştığını kontrol eden mekanizmalar bulunmamaktadır. Daha küçük boyutlu paketlerin iletiminin sağlanması ve veri güvenliğinin öncelikli olmadığı daha düşük bant genişliği gereken durumlarla kullanılmaktadır. TCP protokolünde olduğu gibi IP bilgisi eklenerek iletilmek istenen hedef belirlenir. Daha hızlı iletimin sağlanması gereken video konferans uygulamaları gibi durumlarda kullanılmaktadır. TCP protokolünde güvenlik mekanizmalarının yer alması nedeniyle UDP iletimi daha hızlıdır.

2.1.2.5. ARP (Address Resolution Protocol -Adres Çözümleme Protokolü)

Ağ katmanında istemci ve sunucu arasında gerçekleşen iletimlerde kaynak ve hedefin IP adreslerine ihtiyaç duyulmaktadır. Fakat yerel ağlarda iletim yapılmak istendiğinde hedef cihazın fiziksel adresin (MAC adresi) bilinmesi gerekmektedir.

İki cihaz arasında iletişim kurulmak istendiğinde iletim yapmak isteyen cihaz kendi ARP tablosunda hedef cihazın olup olmadığını kontrol etmektedir. ARP tablosunda hedef cihaz bilgisine ulaşılamadığı takdirde ağda bulunan tüm cihazlara (broadcast) yayın yaparak hedef cihazın MAC adres bilgisini kendi ARP tablosuna ekler. Hedef ve kaynak cihaz arasındaki iletişim bu şekilde sağlanmış olmaktadır.

ARP protokolü kullanılarak gerçekleştirilen saldırı türleri arasında ARP Spoofing veya ARP Cache Poisoning saldırıları yaygın olarak kullanılmaktadır.

2.1.2.6. ICMP (İnternet Kontrol Mesaj Protokolü)

ICMP protokolü ağda bulunan cihazların durumunu, ulaşılıp ulaşılmadığını tespit etmek amacıyla kullanılmaktadır. ICMP TTL (Time To Live) süresinden sonra paketin sahibine bildirim yapma, hata oluşumlarında geri bildirim sağlama ve paket başka bir yoldan gideceği zaman geri bildirim sağlama gibi görevleri bulunmaktadır. Ping ve Tracert komutlarıyla ICMP mesajları çalıştırılmaktadır. ICMP protokolü tracert komutları gibi komutlarla çalıştırılarak bilgi toplama amacıyla kullanılabilmektedir. Güvenlik amacıyla söz konusu komutların kullanımının kısıtlanmasıyla gereken tedbirler alınmaktadır.

2.1.2.7. DNS (Domain Name System–Alan Adı Sistemi)

DNS internet dünyasında varolan web sayfalarına ait IP adreslerine karşılık gelen isimleridir. Bu protokol standart olarak 53 numaralı port üzerinden aktifleştirilmektedir.

Erişim sağlanmak istenen web sayfasına kullanıcılar tarafından gönderilen istek gönderilmesi ile bu protokol başlatılır. Alan adları ve alan adlarına karşılık gelen IP bilgiler DNS sunucularında tutulmaktadır. Kullancılar tarafından istek gönderildiğinde DNS sunucularında alan adına karşılık gelen IP adresine yönlendirme sağlanmaktadır. Alan adı ve IP adres çözümlemesi ilk olarak root (yönlendirme) sunucularında başlamaktadır. Yönlendirme sunucuları gelen istekleri adreslerini bildikleri TLD (Top-Level Domain) sunucularına iletmektedir. TLD sunucuları jenerik ve ülke kodlu alan adları olmak üzere iki gruptan oluşmaktadır. Ülke kodlarının yönetimi ülkeden ülkeye farklılık göstermekte olup Türkiyede yönetimi ODTÜ tarafından gerçekleştirilmektedir. Bir sonraki seviye ise SLD (İkinci Seviye Alan Adı - Second Level Domain) sunucularıdır. Kişilere ve kurumlara göre farklı uzunluklarda alan adlarını oluşturmaktadır (Karimkhani, 2020).

2.1.2.8. SNMP (Basit Ağ Yönetim Protokolü)

Teknolojiyle parallel olarak giderek büyüyen ağlarda yer alan cihazların yönetilmesini sağlayan bir protokoldür. SNMP protokolü ile yönlendirici (router), anahtarlayıcı (switch) gibi ağ cihazlarının çalışma süresi, CPU kullanım seviyesi, bellek kullanımı, cihazlara ilişkin üretim bilgileri (seri numarası), üzerindeki trafik bilgileri olan performans gibi birçok veriye ulaşılabilmektedir. SNMP protokolü ağda bulunan cihazların trafik akışı gibi performans verilerini kontrol etmesi nedeniyle hızlı bir iletim sağlayan UDP protokolünü kullanmaktadır.

SNMP protokolü üç temel bileşenden oluşmaktadır (Tutar, 2020).

- SNMP yöneticisi, ağ yönetimi tarafından kullanılan ve SNMP protokolü ile elde edilen verilerin görüntülendiği bir yazılımdır.
- SNMP ajanı, söz konusu verilerin elde edilmek istenen ağ cihazlarında bulunan yazılımlardır.
- SNMP MIB, ağ cihazları ve ağ yöneticisi arasında bulunan bileşenlerdir.

2.1.2.9. FTP (File Transfer Protocol–Dosya Aktarım Protokolü)

İnternete bağlı bulunan iki bilgisayar arasında dosya aktarımının yapılması için kullanılmaktadır. FTP protokolü ile yapılan dosya transferlerinde iletim sağlanmak istenen bilgisayarın adresi, kullanıcı adı ve şifre bilgileri, internet bağlantısı olan ve FTP yazılımı bulunan bilgisayara ve komutların yorumlanmasını sağlayan FTP istemcisine ihtiyaç bulunmaktadır. Kullanıcıların FTP sunucularına erişiminde kimlik doğrulama mekanizmaları kullanılmaktadır. Ekleme, silme gibi komutları karşı bilgisayarda çalıştırabilemektedir.

2.1.2.10. HTTP (Hyper Text Transfer Protocol–Hiper Metin Aktarım Protokolü)

HTTP, internete bağlı sunucular ve istemci arasındaki iletişimin nasıl kurulması gerektiğini düzenler. HTTP protokolünün çalışma mantığı istek ve cevap başlıkları şeklindedir. İletişim kurmak isteyen istemci istek gönderir ve sunucu bu isteği değerlendirerek cevaplamaktadır.

2.1.2.11. SMTP (Simple Mail Transfer Protocol–Basit Posta Aktarım Protokolü)

Sunucular arasında e-posta gönderiminde kullanılan bir protokoldür. Alıcı tarafta mesajların sıralanmasını sağlayan POP3 ve IMAP protokolleriyle birlikte kullanılmaktadır. SMTP protokolü e-postayı gönderen sunucu, alan sunucu ve istemci arasında görev almaktadır. İlk aşamada gönderim yapılmak istendiğinde

gönderen SMTP protokolü kullanılır. İkinci aşama olarak gönderen e-posta sunucusu alıcı e-posta sunucusuna SMTP ile göndermektedir. Son aşama olarak alıcı sunucu e-posta mesajını POP3 veya IMAP indirmek için e-posta istemci olan Outlook kullanmaktadır (Hosting, 2020).

2.1.2.12. DHCP (Dinamik Bilgisayar Konfigürasyon Protokolü)

Birçok cihazın bağlı olduğu ağlarda sabit bir IP vermek yerine daha hızlı IP verilebilmesini sağlayan bir protokoldür. Ağa bağlı cihaz farklı alt bir ağa taşınmak istendiğinde ana makineye bağlı olarak IP adresinin değiştirilmesi gerekmektedir.

DHCP istemci sunucu mantığıyla çalışan bir sistemdir. Taşıma katmanında UDP protokolünü kullanmaktadır. İstemci ağa keşif (discovery) paketleri göndererek DHCP sunucusunu bulmaya çalışır. Keşif paketini alan DHCP sunucusu ise söz konusu paketi gönderen istemciye IP adresi ve kullanabileceği IP adresini ne kadar süre kullanabileceğini belirleyen paket gönderir. Belirlenen IP adresini alan istemci ise belirlenen IP ve süreyi kabul eden bir cevap paketi (DHCP Request) gönderir. İstemciye verilen sürenin bir kısmı dolduğunda istemci DHCP sunucusuna IP adresinin yenilenmesini isteyerek verilen sürenin uzatılmasını sağlar. İsteğe DHCP sunucusu cevap vererek bu süre zarfında ilk IP adresinin korunması sağlanmış olur.

2.1.2.13. POP (Post Office Protocol–Posta İletim Protokolü)

Güncel versiyonu POP3 olan protokol TCP portunu kullanarak istemcinin yerel bir makinede, sunucunun ise uzak bir makinede çalışmasına olanak sağlamaktadır. POP3 protokolü uzak POP3 sunucusundan e-mail alarak yerel POP3 istemcisine getirmek ve istemcinin sunucu üzerinde belirli komutlar çalıştırarak e-mailleri yönetmesini sağlamaktadır.

3. AKTİF VE PASİF SALDIRI TÜRLERİ

3.1. Saldırı Türleri

Kurum veya şirketlerin iç veya dış ağlardan meydana gelebilecek potansiyel riskler ile güvenlik fonksiyonlarının durma noktasına getirilebilmesi ihtimali tehdit olarak adlandırılmaktadır. Tehditlerden yararlanılarak meydana gelen ve güvenlik sistemlerinin durmasına neden olan olaylar ise siber saldırı olarak tanımlanmaktadır. Kurumların itibarsızlaştırılması, parasal kaynakların elde edilmek istenmesi gibi birçok farklı motivasyon sağlayan kötü niyetli kişiler tarafından yapılan aktif ve pasif saldırı türleri aşağıda incelenmiştir.

3.1.1 Paket Koklama

Pasif ve aktif her iki sınıf içerisinde bulunnan paket koklama ile hedef sistemin ağ paketleri yakalanarak analiz edilmesi neticesinde email, web, SMB ftp, telnet, SQL içerisinde bulunan şifrelerin ele geçirilmesi ve sistem hakkında bilgi sahibi olunması amaçlanmaktadır. Paket koklama yöntemi ile kişisel veriler, şifreler, VOIP hatları üzerinden yapılan telefon görüşmeleri, ağ topolojisine ilişkin bilgi edinimi ve işletim sistemleri hakkında bilgi sahibi olma gibi hedefleri de bulunmaktadır. Telnet, http, SMTP, POP, FTP protokolleri paket koklama yönetiminde kullanılabileceği için söz konusu protokollere yönelik güvenlik önlemlerinin alınması sağlanmalıdır.

3.1.2 Aldatma (Spoofing)

Aldatma yöntemi saldırganın kendini başka bir adres ve kimlik bilgileri ile gerçekleştirdiği saldırı türüdür. Hedef sistemin güvenebileceği bir kimlik bilgisine bürünmesi nedeniyle tespit edilmesi zor bir saldırıdır.

3.1.3. IP Aldatmacası (IP Spoofing)

Gelen paketlerin kaynak IP adreslerinin değiştirilmesi ile sağlanmaktadır. Kaynak IP adresi değiştirildiğinde güvenilir bir kaynaktan geldiği düşünülmektedir. IP adresilerine göre iletim sağlayan servisler bu saldırıdan oldukça etkilenmektedir. KOD, Jolt, Papasumurf gibi yazılımlar IP aldatmaca saldırısında kullanılmaktadır.

3.1.4. MAC Aldatmacası (MAC Spoofing)

MAC aldatmacası yöntemiyle her bir cihaza özel verilen 48 bitlik uzunluğunda eşsiz MAC adresinin hedef ağ içerisinde bulunan güvenilir bir cihaz adresiyle değiştirilerek saldırgan varlığını gizleyebilmeyi sağlamaktadır.

3.1.5. ARP Önbellek Zehirlenmesi

Ağa bağlı sistemlerin birbirleriyle iletişim kurabilmesi kendilerine ait fiziksel ve mantıksal adres ile mümkün olabilmektedir. Yerel ağlar içerisinde kullanılan anahtarlama (switch) cihazları üzerinden geçen trafiği yönlendirmek için ağa bağlı bilgisayarların fiziksel adres (MAC) bilgisine ihtiyaç duymaktadır. Ağ içerisinde bulunan bilgisayarlar mantıksal IP adresini bildikleri bilgisayarların fiziksel adreslerini (MAC) ARP tablousu üzerinden öğrenmektedir. Böylelikle ARP protokolü, fiziksel adres ve mantıksal adres arasındaki bağlantıyı kurar. Mantıksal IP adresi bilinen bilgisayarın fiziksel adresi ARP tablosunda yoksa tüm ağdaki bilgisayarlara iletişim kurulmak istenen bilgisayarın fiziksel adresini öğrenmek için ARP Request paketleri iletilir.ARP zehirlenmesi ise saldırganların ARP tablosunda yer alan IP ve MAC eşleştirmelerinde kendi MAC adreslerini hedef bilgisayarın MAC adresiyle değiştirmesi sağlanarak trafiği kendi üzerine yönlendirmesi mümkün olmaktadır. Saldırgan bu şekilde araya girerek hattı dinleme ve değiştirme eylemlerinde bulunabilmektedir.

3.1.6. DNS Zehirlenmesi

Hedef bilgisayarda bulunan zararlı yazılımlar ile DNS sunucusuna gelen tüm trafik saldırgana ait olan makineye yönlendirilerek trafiğin izlenmesi, veri paketlerinin ele geçirilmesine neden olabilmektedir. Saldırıya uğrayan bilgisayar örnek olarak google adresine gittiğini düşünürken saldırganın yönlendirdiği farklı bir adrese gitmektedir. Bu nedenle saldırının farkedilmesi oldukça zordur. Saldırganın tüm trafiği izlemesi mail, sosyal medya hesapları, internet bankacılığı gibi birçok sayfadan giriş yapılan hesap bilgilerini geçirmesine neden olmaktadır.

3.1.7. Dağıtık Hizmet Engelleme Saldırıları (DDOS)

Saldırganlar tarafından kötü amaçlı yazılımlar ile ele geçirilen bilgisayarlar botnet olarak adlandırılmaktadır. Botnet adı verilen bilgisayarların uzaktan kontrol edilerek eş zamanlı hedef bir sisteme yaptıkları sistemin çevrimiçi hizmetinin sınırlandırılması veya durdurulması amacıyla yaptıkları saldırılar dağıtık hizmet engelleme sadırılarıdır. Günümüzde oldukça yaygın bir saldırı yöntemi olan DDOS web sitelerinin sunucuları arasındaki bağlantının kopması, sunucu kaynak tüketiminde yoğunlaşmaların meydana gelmesi, UDP, SYN ve GET/POST kaynaklı yığılmalar, uzun süreli hizmet kesintileri, web sayfalarında donmalar gibi kayıplara neden olmaktadır. Saldırgan sistemi erişilemez duruma getirerek itibar kaybı, maddi kayıp gibi nedenlere yol açmayı amaçlamaktadır. DDOS saldırılarına yönelik geliştirilen IDS ve IPS sistemleri ile saldırılar tespit edilerek hızlı bir şekilde önlenmektedir. DDOS saldırıları engelleme sistemlerinde yedek bir hat oluşturularak trafiğin diğer hat üzerinden devam etmesi sağlanmaktadır.

3.1.8. SYN Taşması

SYN taşması yaygın olarak kullanılan bir hizmet engelleme saldırı çeşididir. TCP protokolünün kullandığı üçlü el sıkışma yönteminde haberleşmek isteyen iki bilgisayar arasında gönderilen SYN/ACK paketleri kullanılarak gerçekleştirilir.

Hedef sunucuya sürekli olarak gönderilen SYN paketlerine bağlantı için sunucunun ACK paketi göndermeye çalışması belirli süre sonra kapasite aşımına neden olmaktadır. Bu yöntem ile hedef sistem erişilemez duruma getirilmektedir.

3.1.9. Hijacking Atağı

Saldırgan sunucu ve kullanıcı arasına girerek kullanıcının oturumunu ele geçirmeyi amaçlamaktadır. Replay ve araya girme teknikleri söz konusu atağın gerçekleşmesinde kullanılmaktadır.

3.1.10. UDP Taşması

UDP taşması saldırganın hedef sunucunun tüm portlarına UDP paketleri göndermesi ile sunucunun kapasitesinin dolmasına neden olan saldırı yöntemidir. Böylelikle yeni gelen isteklere sunucu cevap vermez hale getirilir.

3.1.11. DNS Taşması

Saldırgan tarafından sunucuya sürekli olarak gönderilen istekler sunucunun istekleri cevaplayamaz hale gelmesine yol açmaktadır.

3.1.12. MAC Taşması

Aktif dinleme yöntemi olarak kullanılan saldırı yöntemleri arasında yer almaktadır. Saldırganın ard arda göndermiş olduğu sahte MAC adresleri, MAC adres tablosunun dolmasına neden olmaktadır.

MAC taşması saldırısına karşı alınabilecek güvenlik önlemleri IP-MAC eşleştirmelerini giriş yerine göre eşleştirilmesi ve birim sürede gelen ARP isteklerini bellirli bir seviyede tutulması ile birim sürede gelen ARP isteği miktarını geçen trafiğin ARP saldırısı olarak algılanmasını sağlamaktır.

3.1.13. HTTP GET/POST Taşması

Saldırganın web sayfasına ait sunucuya sürekli olarak GET ve POS mesajları göndermesi sunucunun söz konusu mesajlara cevap veremez hale gelmesine neden olmaktadır.

3.1.14. Brute Force Atakları

Bir tür parola yakalama yöntemidir. Saldırgan kullanılan kötü amaçlı yazılım ile karakter kombinasyonlarını deneyerek parolayı tahmin etmeye çalışır. Hedef sistemin içerisinde bulunan hesap bilgilerine ait parolaların kısa ve basit olmaması güçlü bir parolanın oluşturulması saldırganın ele geçirmesini önleyebilemektedir.

3.1.15. Zararlı Kod Atakları

Kod atakları, özel yazılmış yazılımlar ile hedef sistemlere zarar vermeyi amaçlamaktadır. Virüs, worm, trojen horses, rootkits, logic bomb, spyware, adware zararlı yazılımlar arasında yer almaktadır. Virüsler, bir dosyaya bulaştığında aktif hale gelerek verileri bozar veya değiştirir.Kendi kendilerine çalışmamaktadır. Worm ise kendi kendine çalışabilen ve hedef bellekte aktif olarak kalan programlardır. Trojen horse (truva atları), virüsler gibi bir hosta ihtiyaç duymayan programlardır. Amacı hedef sistemden dışarıya bilgi sızdırmaktır. Rootkit, kendilerini gizleyebilen iştetim sisteminin temel bileşenlerini bozmayı hedefleyen, sistemin kontrolünü ele geçirmeye çalışan programlardır. Logic Bomb, saldırgan tarafından hedefe gönderilmeden önce tarih ve zaman ayarı yapılmış yazılımlardır. Sisteme girdikten sonra belirtilen zamanda aktif hale gelmektedir. Spyware ve Adware yazılımları ile hedef sistemden bilgi sızdırmak amaçlanmıştır.

3.2. Ağ Keşifleri

Ağa bağlı olarak bulunan cihazların model bilgileri, IP bilgileri, cihaz üzerinde bulunan işletim sistemi bilgileri gibi ağın topolojisi hakkında birçok veriye ağ keşifleri yöntemleriyle ulaşılabilmektedir.

3.2.1. IP Tarama

IP tarama ile ağda aktif olarak çalışan cihaz bilgisine erişebilmektedir. Bu yöntemde ping komutu gönderen saldırgan hedef cihazdan ICMP echo replay paketlerinin dönüp dönmediğini konrol etmektedir.

3.2.2. Port Tarama

TCP, IP, ICMP, UDP gibi protokollerin yardımıyla açık port tespiti mümkündür. Birçok port tarama teknikleri bulunmaktadır.

TCP Connect/Full Open Scan (TCP Bağlantı/Açık Tarama) yöntemi üçlü el sıkışma yöntemiyle port açık olduğunda tespit edebilmektedir. Port kapalı durumdaysa RST paketi ile dönüş yapmaktadır (Şen, 2020).

Stealth Scan/Half-open Scan (Gizli Tarama/Yarı Açık Tarama), üçlü el sıkışma yöntemi tamamlanmadan hemen önce sunucu ve istemci arasındaki TCP bağlantısına reset atarak güvenlik duvarı ve loglama mekanizmaları tarafından tespit edilmesini önlemektedir (Şen, 2020).

Inverse TCP Flag Scanning (Ters TCP Bayrağı Tarama) yönteminde iletilen TCP bayrağıyla veya bayraksız araştırma paketleri (probe packets) gönderilmesi sonucunda cevabın gelmemesi portun açık olduğunu, RST dönüşünün olması ise kapalı bir port olduğu belirtmektedir.

3.2.3. Uygulama ve açık taraması

Uç sistemlerde kullanılan firewall, router, switch gibi ağ cihazları ve ağda yer alan cihazların işletim sistemleri üzerinde çalışan yazılımlarında bulunan açıkları tespit edebilmek amacıyla gerçekleştirilmektedir.

3.2.4. Siber tehditlere ilişkin alınan önlemler

Kurumsal ya da bireysel yaşamımızda internetten gelebilecek saldırılara açık halde bulunan bilgi sistemlerinin korunmasına yönelik VPN teknolojileri ve Firewall (Güvenlik Duvarı) kullanılmaktadır.

VPN: Günümüzde birçok kurum farklı noktalarda bulunan çalışanları veya bağlı ortaklarıyla veri iletimi, video konferans, ses iletimi gibi birçok alanda haberleşme istediği duymaktadır. Bu teknoloji ile bağlantı yapılmak istenen iki nokta arasında kurulan tünelleme ile verinin kriptolu olarak gönderilmesi sağlanmaktadır. Araya girmeye çalışan saldırgan verinin şifrelenmiş olması nedeniyle ele geçirmesi imkansız hale gelmektedir.

Güvenlik Duvarı: Kurumsal veya bireysel internet kullanımında belirlenen erişim kurallarına uygun olan trafiğin kabul edilmesini uygun olmayan trafiğin ise engellenmesini sağlayan cihazlardır. Güvenlik duvarı arayüzünde uygulama olarak veya ip adres bilgi verilerek kurumların politikalarına uygun kurallar oluşturulabilmektedir. Fakat güvenliğin sağlanmasında dışarıdan gelebilecek tehditleri kısıtlasa da bu teknolojiler yapılan siber saldırıların tespit edilmesinde yetersiz kalabilmektedir.

4 SALDIRI TESPİT SİSTEMLERİNİN ÖNEMİ

Meydana gelebilecek saldırıların tespit edilmesi için ağda gerçekleşen aktivitelerin izlenmesi ve analiz edilmesi ile kısa bir zaman içerisinde gerekli önlemin alınmasında STS'ler önemli görev üstlenmektedir.

4.1. Saldırı Tespit Sistemlerinin Bilgi Güvenliğinde Önemi

4.1.1. Saldırı Tespit Sistemi

Bilgi sistemlerine yapılan saldırıların tespit edilmesi ve engellenmesine yönelik tasarlanmış sistemler olan saldırı tespit sistemleri (STS) bilginin ağ ortamında taşınırken, işlenirken veya depolanırken maruz kalabileceği tehdit ve tehlikelerin ortadan kaldırılması amacıyla, bilgiye yetkisiz erişim veya kötüye kullanımı gibi girişimleri tespit edebilen, saldırının sistem güvenliğinden sorumlu kişiye iletebilme özelliğine sahip yazılımsal/donanımsal güvenlik araçlarıdır. Ağ cihazlarını izleyerek anormal davranışları da tespit edebilmektedir (Baykara ve Daş, 2019, s. 59).

4.1.2. Saldırı Tespit Sistemlerinin tarihçesi

Saldırı tespit sistemi kavramı ilk olarak Anderson tarafından "Bilgisayar Güvenliği Tehdit Gözetleme ve İzleme (Computer Security Threat Monitoring and Survaillance) 1980 yılında ortaya atılmıştır. Anderson yayımlanan makalesinde yetkisiz erişimlerin denetim izleriyle tespit edilebileceğinden bahsetmektedir (Anderson , 1980, s. 2).

Saldırı tespit sistemlerinin ilk modellerinde basit bir yapı bulunurken ikinci nesil modellerde denetim izi kavramı da yer almaktadır. Günümüzde saldırı tespit sistemlerinde istatiksel verilerin yer aldığı ve yapay zeka teknolojilerinin kullanıldığı bir sistem haline olarak karşımıza çıkmaktadır.

4.1.3. Saldırı Tespit Sisteminin neden gereklidir?

Gelişen teknoloji ile birlikte sistemlerin birbirileriyle bağlantısının artması ve dış ağlara açık durumda bulundurulması gerekliliği saldırıların artmasına da neden olmaktadır. Bu sebeple güvenilir bir sistem oluşturulma gerekliliği aşağıda ifade edilmektedir (Güven, 2007a).

1. İşletim sistemi açıklıklarının saldırganlar tarafından tespit edilmisi ve kötü niyetli olarak kullanılması
2. OSI katmanlarında veri iletimi için kullanılan protokollerin işleyisinden kaynaklı bulunan bazı kuralların kötücül amaçlı istismar edilebilmesi
3. Şifreleme yöntemlerinin ve kullanıcıların şifre teknikleriyle ilgili olarak yaşadıkları sorunlar nedeniyle yüksek seviyede güvenliğin sağlanamaması
4. Dış ortamlara karşı korunan sistemlerin iç ortamlardan kaynaklanan güvenlik zafiyetine uğrayabilmesi
5. Kullanılan güvenlik mekanizmalarının, olası yeni saldırıları tespit edebilecek şekilde güncellenmemesi
6. Bilgi güvenliğinin sağlanması için gereken güvenlik politikalarının doğru olarak belirlenip uygulanmaması
7. Güvenlik amacıyla kullanıcı yetkilerinin minimuma indirilmesi nedeniyle kullanıcı verimliliğinin düşmesi

4.2. Saldırı Tespit Sistemlerinin Kullanılmasının Avantajları

STS'leri saldırının tespit edilmesi, sistemin güvenliğinin sağlanması hususunda vazgeçilmez bir sistem olmalarının nedenleri aşağıda belirtilmiştir (Bace, 1999).

1. Sistemin güvenlik alt yapı bütünlüğünün sağlanmasına katkıda bulunur.
2. Kullanıcı davranışlarını izler ve gerektiğinde müdahele edebilir.
3. Sistemde varolan verilerdeki değişiklikleri algılayarak rapor düzenler.
4. Güvenlik zafiyetine neden olabilecek konfigürasyon hatalarını bularak hataları düzeltebilir.

5. Sistemin maruz kalabileceği saldırıları tahmin eder.
6. Yeni saldırı türlerini öğrenerek hafızasında tutar.
7. Yönetilmesi kolay bir arayüze sahiptir.

Bilginin korunmasını isteyen kurumların ya da kişilerin kullanmak istedikleri sistemlerin saldırıların hızlı bir şekilde tespit edilerek önlenmesini ve yeni saldırıları öğrenerek önlem alınmasını istemeleri saldırı tespit sistemlerini oldukça cazip hale getirmektedir.

4.3. Saldırı Tespit Sistemlerinin Mimari Yapısı

STS'lerin mimari yapısı ağ üzerinde konumlandırıldıkları yer, bilgi sistemlerine ilişkin temel fonsiyonel bileşenler ile nasıl konumlandırıldıklarıyla ilgilidir. Temel fonsiyonel bileşenler; izlenen sistem, analizin yapıldığı sunucu ile çevresi, ağ cihazları ve problemler için izlenen hedef olarak verilebilir (Baykara, 2016a).

STS'ler mimari yapı açısından, "merkezi sistem" ve "dağıtık sistem" olmak üzere ikiye ayrılmaktadır. Merkezi sistem mimari yapısında; tüm izleme, tespit ve raporlama işlemleri bir merkezde kontrol edilir. Bilinen STS'lerin büyük bir kısmı bu kategoriye girer. Merkezi kontrol için fiziksel yakınlık önemli bir etken değildir (Baykara, 2016b).

4.4. Saldırı Tespit Sistemlerinde Kullanılan Yöntemler

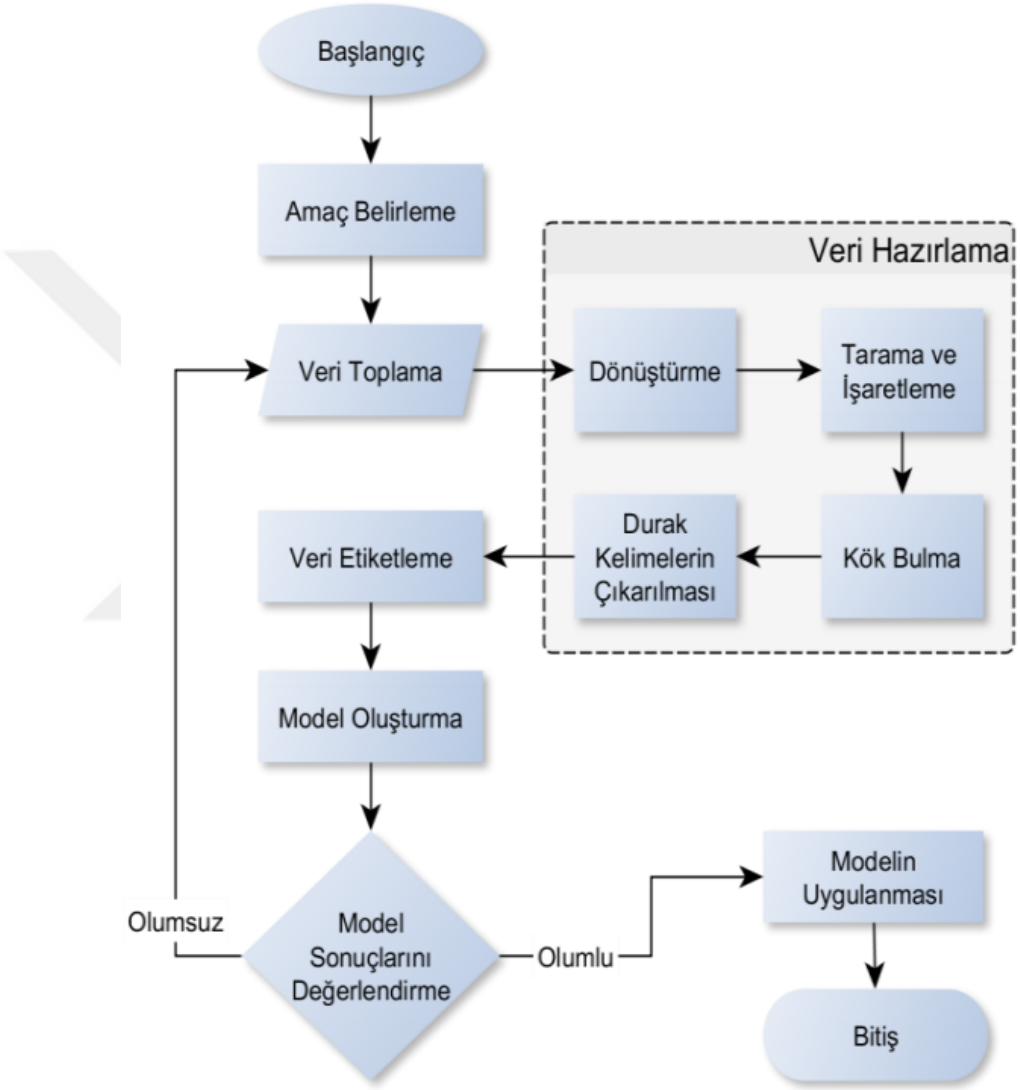
Saldırıları tespit etmek amacıyla kullanılan yöntemlerden bazılarına aşağıda yer verilmiştir.

4.4.1. Metin Madenciliği (Text Mining)

2000'li yıllardan sonra popular hale gelen metin madenciliği veri madenciliği, makine öğrenmesi, istatistik ve işlemsel dilbilim kavramlarıyla ortak bir çalışma alanıdır (WikiPedia, 2020). Oldukça büyük boyutlarda bulunan ham veriler

sınıflandırma, gruplandırma yöntemleriyle analiz edilerek gerekli bilgiler elde edilmektedir.

Metin sınıflandırma süreci ise Şekil 4.1'de gösterilmiştir (Kaşıkçı ve Gökçen, 2014, s. 26).



Şekil 4.1 Metin Madenciliği sınıflandırma aşamaları

4.4.2. Veri Madenciliği (Data Mining)

Veri madenciliği; daha önceden bilinmeyen, geçerli ve uygulanabilir verinin ham verinin içerisinden elde edilmesi yöntemidir. Bu süreçte kümeleme, veri

özetleme, veriler arasındaki ilişki, anomali tespiti gibi birçok teknik kullanılmaktadır (Baykal, 2006, s. 96).

Veri madenciliği bankacılık, pazarlama, sigortacılık, bilgi teknolojileri gibi birçok alanda veri tabanı analizi, risk analizi, saldırı tespiti gibi verilerin elde edilmesi için bir aşama olarak kullanılmaktadır.

4.4.3. Toplama Yöntemi (Ensemble Method)

Toplama Yöntemi makine öğrenmesi yöntemleri arasında yer alan bir algoritmadır. Diğer makine öğrenme yöntemlerinin yeterince ele almadığı veri setinde yer alan dengesizliklerin giderilmesinde kullanılmaktadır. Bu yöntem; güçsüz algoritmaları birleştirerek tahminlerin daha güçlü yapıldığı, doğruluk oranı yüksek bir algoritma oluşturmaktadır.

Anazida Zainal ve arkadaşları toplama tekniği ile Rasgele Orman (Random Forest) algoritması kullanarak Prob, DoS, U2R ve R2L saldırılarında yüksek doğruluk oranı elde etmişlerdir (Zainal vd., 2009, s. 217).

4.4.4. Kural Tabanlı (Rule Based) Sistemler

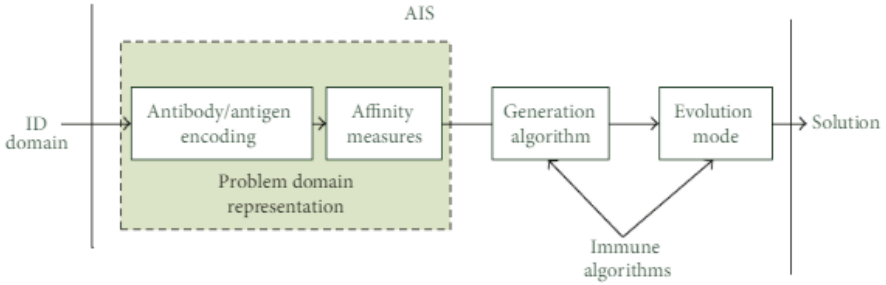
Kural tabanlı STS'ler ağ trafiğinin incelenmesi sonucunda veri tabanında yer alan kurallara göre gelen veriyi analiz eder.

En yaygın kullanılan yöntem olan kural tabanlı sistemler imza bilgileri doğru olduğunda ve kurallar bir iyi bir uzman tarafından oluşturulduğunda en iyi performansı göstermektedir (Turner vd., 2016, s. 361).

4.4.5. Bağışık Sistemler (Immune Systems)

Son zamanlarda oldukça sık kullanılan bir saldırı tespit yöntemi olan bağışık sistemler anormal davranışların tespit edilmesinde oldukça başarılı sonuçların ortaya çıkmasını sağlamaktadır.

Bağışık Sistem tabanlı bir saldırı tespit sisteminde canlıda meydana gelen bağışıklık sisteminde olduğu gibi anormal davranışlar için antijen olarak nitelendirilen bir veri bulunmaktadır. Antijen /Antikor kodlaması, üretim algoritması ve evrim modu olarak üç aşamadan oluşan bir sistemdir. Şekil 4.2'de Bağışık sistem tabanlı saldırı tespit sistemine ilişkin genel yapısı verilmiştir. (Yang vd., 1-11, s. 2).



Şekil 4.2 Bağısık Sistem Tabanlı STS tasarımı için framework yapısı

4.4.6. Uzman Sistemler (Expert System)

1970'li yıllarda yapay zeka alanında araştırmacılar tarafından geliştirilmiş uzman sistemler problemleri çözüme kavuşturan düzeltmeleri yapmak için bir iş dizisi öneren zamanla kendini geliştirme yeteğine sahip olan yazılımlardır (WikiPedia, 2020).

Dorothy E. Denning ve arkadaşının yardımıyla, bugün birçok sistemin temelini oluşturan bir saldırı tespit sistem modelini 1986'da yayınlanmıştır. Bu model anomalilik tespiti için istatistik kullanarak hem ağ hem de kullanıcı düzeyinde analiz gerçekleştiren uzman sistem olarak tanımlanmaktadır (Denning, 1986; Lunt, 1990).

4.4.7. Açıklayıcı İstatistikler (Descriptive Statistics)

Açıklayıcı istatistik temelli STS'ler kullanıcının ya da sistemin davranışlarını izleyerek bir model meydana getirmektedir. Disk alanı, oturum girişi, oturum

kapatma, hafıza alanı, dosya sayısı gibi çeşitli değişkenler kullanılarak oluşturulan modelde sistem üzerindeki davranışlar sürekli olarak ölçülmektedir (Baykara, 2016, s. 64).

Çizelge 4.1'de Saldırı Tespit Sistemlerinde kullanılan yöntemlerin karşılaştırılmasına yer verilmiştir (Güven, 2007b; Sancak, 2008).

Çizelge 4.1 STS'lerde kullanılan tekniklerin karşılaştırılması

Teknik	Tespit Yaklaşımı	Bilgi Kaynağı	Bilinen Saldırı	Bilinmeyen Saldırı	Başarım
Metin Madenciliği	Anormallik	Denetim verisi, Bilgi tabanı, Log kayıtları	Evet	Evet	Orta
Veri Madenciliği	Anormallik	Denetim Verisi, Bilgi Tabanı	Evet	Evet	Orta
Ensemble	Anormallik	STS Bilgi Tabanı	Evet	Evet	Orta
Uzman Sistemler/ Kural Tabanlı	Kötüye Kullanım	Kural Bilgi Tabanı	Evet	Hayır	Yüksek
Bağışık Sistemler	Anormallik	Denetim Verisi, Bilgi Tabanı	Evet	Hayır	Yüksek
İstatistiksel	Anormallik	Denetim Verisi, Kullanıcı Profili	Evet	Evet	Orta

4.5. STS'lerde Algılama Yöntemleri

4.5.1. Anomali Tabanlı Saldırı Tespit Sistemleri (Anomaly Based IDS)

Saldırı tespit sistemlerinde anomali tabanlı ve imza tabanlı iki farklı yaklaşım bulunmaktadır (Anderson vd., 1995). Anomali tabanlı saldırı tespit sistemleri sistemin yapısını incelenerek meydana gelen normal durumları hafızasına kaydetmektedir. Normalin dışında gelen olayları analiz ederek saldırı olup

olmadığına karar verebilmektedir. Bu yaklaşım daha önce gerçekleşmemiş saldırıları da tespit edilmektedir. Saldırı olmayan davranışların anormal davranışlara yakın özelliklere sahip olması yanlış alarm (false positive) oluşmasına neden olabilmektedir. Anormal davranışların tespitinde makine öğrenme metotları, veri madenciliği, bilgi kuramı, istatistik gibi birçok araştırma alanı ve farklı teknik kullanılmaktadır.

4.5.2. İmza Tabanlı Saldırı Tespit Sistemleri (Signature Based IDS)

İmza tabanlı saldırı tespit sistemlerinde veriabanına daha önceden kaydedilmiş saldırıların imzasına sahip olan saldırıları tespit edilmektedir. Veritabanında bulunmayan yeni bir saldırıyı tespit edemez.

4.5.3. Örüntü Eşleştirmeli STS (Pattern Matching IDS)

Saldırı tespit sistemlerinde kullanılan algoritma paket dizisi içerisinde yer alan imzanın varlığını kontrol etmektedir. Tekli ve çoklu model eşleştirme algoritmaları olarak iki ayrı yaklaşımı kullanılmaktadır. Tekli eşleştirme algoritması bir seferde tek örüntüyle eşleştirir fakat çoklu eşleştirme algoritması aynı anda tüm imzalarla karşılaştırmaktadır. Ancak, çoklu eşleştirme algoritması daha fazla belleğe ve ön işlemeye ihtiyaç duymaktadır (lnxmaster, 2020).

4.5.4. Durumsal Örüntü Eşleştirmeli STS

Sisteme gelen paket içerisinde daha önceden belirlenen bayt dizilerinin kontrol edilmesiyle saldırı tespiti yapılmasında kullanılan bir yöntemdir. Sistem içerisinde fazla belleğe ihtiyaç duyan bu yöntem örtüntü eşleştirme yöntemine göre daha yavaştır fakat daha çok false – positive alarm üretebilmektedir (lnxmaster, 2020).

4.5.5. Kod Çözme Protokol Tabanlı Analiz (Protocol Decode - Based Analysis)

Saldırı tespit sistemleri tarafından tanımlanan protocol ihlallerini arayarak false – positive alarmları azaltmada etkili olarak kullanılmasına rağmen tanımlanan protokolleri gözden kaçırabilmektedir (Akkaya, 2020).

4.5.6. Sezgisel Temelli Analiz (Heuristic-Based Analysis)

Daha önce tanımlanan ve imzası oluşturularak veribanına kaydedilen zararlı yazılımlarla karşılaştırma yapılarak tespit edilmesinde kullanılmaktadır. Sezgisel analiz yöntemi şüpheli yazılımın kaynak kodunu çözerek inceler ve sezgisel veritabanında bulunan virüslerle karşılaştırır (lnxmaster.com, 2020) .

4.6. Bilgi Kaynaklarına Göre STS'lerin Sınıflandırılması

4.6.1. Ağ Temelli STS'ler

Bir sistemin merkezi noktalarına yerleştirilen saldırı tespit sistemleri ile alt ağların dahil olduğu çift yönlü(gelen/giden) trafik merkezi bir konumdan analiz edilir. Bilenen atakların kaydedildiği kütüphanede bulunan verilerle eşleştirilerek saldırının tespit edilmesi durumunda yöneticiye uyarı (alarm) gönderilir. Çevrimiçi ve çevrim dışı ağ tabanlı saldırı tespit sistemi olarak iki çeşidi bulunmaktadır. Çevrimiçi ağ tabanlı saldırı tespitinde gerçek zamanlı olarak ethernet paketleri analiz edilerek gerekli kurallar uygulanır. Çevrimdışı ağ tabanlı saldırı tespit sistemlerinde ise depolanan veri incelenerek saldırı olup olmadığına karar verilir (Vikipedi, 2020).

4.6.2. Dağıtık Temelli STS'ler

Saldırıların daha hassas tespit edilmesi için kullanılan dağıtık mimari merkezi yaklaşımların sınırlamalarını aşmak için mobil ajan sistemleri ile kullanılmaktadır. Ajanlar tek bir noktadan kontrol edebildiği için aralarında bir

dizilim bulunmamaktadır. Diğer ajanlardan bağımsız hareket ederek bu sayede farklı görevleri yerine getirebilmektedir (Söğüt vd., 2017).

4.6.3. Sunucu Temelli STS'ler

Sunucu temelli saldırı tespit sistemleri bilgisayar üzerinden toplanan verilerle tespit edebilmektedir. İşletim sistemlerine yapılan saldırıları sistem günlükleri ve uygulama kayıtları ile doğrudan temin edebilmektedir. Yüksek doğruluk ve güvenilirlik sağlarlar. Anahtarlamalı ağlar üzerinde daha verimli çalışmaktadır. Yerel sunucuları izleme yetenekleri ile ağ temelli STS'lerin yakalayamayacağı saldırıları tespit edilirler. Truva atları veya yazılım eksikliklerinden dolayı gerçekleştirilen saldırıları tespit etme özellikleri bulunmaktadır (Aydın, 2005, s. 12).

4.6.4. Uygulama Temelli STS'ler

Uygulama temelli saldırı tespitinde kullanılan yazılım uygulaması ile meydana gelen olayları analiz eden sunucu temelli STS'lerin özel bir türüdür. Bilgi kaynağı olarak genellikle uygulamaya ait günlük dosyalar kullanılır. Uygulamalara ilişkin özelliklerin belirtildiği takdirde yetkisini aşan kullanıcıların gerçekleştirdiği saldırılar uygulama temelli saldırı tespit sistemleriyle tespit edilebilmektedir (Bace, 2001).

4.6.5. STS'lerde kullanılan metrikler

Saldırı tespit sistemleri tarafından bilgi kaynağından elde edilen verilerin değerlendirilmesi aşamasında kullanılan metrikler aşağıda yer almaktadır.

Doğru pozitif (True Positives): Sınıflandırılması doğru kabul edilen saldırılar için kullanılmaktadır.

Doğru negatif (True Negatives):Gerçekte saldırı olmayan, yanlışlıkla saldırı olarak sınıflandırılan davranışlardır.

Yanlış pozitif (False Positives): Saldırı olmayan aktivitelerin yanlışlıkla saldırı olarak sınıflandırılmasıdır.

Yanlış negatif (False Negatives):Gerçekte saldırı olan aktivitelerin saldırı olarak değerlendirilmemesidir.

4.7. Saldırı Tespitinde Kullanılan Araçlar

Teknolojinin gelişmesine paralel olarak yapılan saldırılara karşı güvenliğin sağlanması gereksinimi bu konuda yapılan çalışmaların artmasına neden olmaktadır. Gerek akademik olarak gerekse ticari olarak yapılan birçok STS yazılımları mevcuttur. Haystack, MIDAS, IDES, W&S, NSM, NADIR, Hyperview, DIDS, USTAT, IDIOT, Ripper, Snort ve Snortsam saldırı tespitinde kullanılan araçlar arasında yer almaktadır.

4.7.1. Haystack

Haystack, 1988 yılında Amerikan Hava Kuvvetleri tarafından kullanılan OS/1100 işletim sistemi içerisinde yer alan çok kullanıcılı ana bilgisayarlar için tasarlanmış bir saldırı tespit sistemidir.

6 farklı saldırı tespitine yönelik geliştirilen STS'nin tespit edebildiği saldırılar aşağıda yer almaktadır. (Güven, 2007b)

- Kırma girişimleri (attempted break-ins)
- Kılık değiştirilen saldırılar (disguised intrusion)
- Güvenlik kontrol sistemine sızma (penetration of the security control system)
- Sızma (leakage)
- Hizmet aksattırma (denial of service)
- Kötü niyetli kullanım (malicious use)

4.7.2. MIDAS

MIDAS (Multics Intrusion Detection and Alerting System), NCSC (Ulusal Bilgisayar Güvenlik Merkezi Bilgisayar Bilimleri laboratuarı (Computer Science Laboratory) ve SRI (Stanford Araştırma Enstitüsü) tarafından NCSC'nin ağa bağlı ana bilgisayarına yönelik saldırıları sezgisel saldırı tabanlı tespit eden bir yazılımdır (Axelsson, 2000a).

4.7.3. IDES

IDES (Intrusion Detection Expert System), Denning ve Neuman'ın 1985'li yıllarda yaptıkları çalışmalar ile geliştirilmiş bir yazılımdır. Kullanıcıların davranışlarını ve kullanıcı hareketlerini normal olarak kabul ederek her gün söz konusu davranışları inceleyerek kendini güncelleyen uzman sistemlerden oluşmaktadır. Daha önceki yapılmış saldırıları hafızasında tutarak kuruma özel politikalar geliştirir (Peddabachigari, 2007, s. 132).

4.7.4. W&S

W&S (Wisdom and Sense–Hikmet ve His), anomali tabanlı saldırı tespit sistemidir. Sistem üzerindeki geçmişe yönelik denetim izleri ve verileri inceleyerek normal davranış örüntüsünü oluşturmaktadır (Vaccarro, 1989).

4.7.5. NSM

NSM (Network Security Monitor), ağı dinleyerek kullanıcı profilleri hakkında bilgi edinerek elde edilen verilerle beklenen bağlantı verilerini karşılıştırır. Bu şekilde beklenen aralıkta bulunmayan davranışları anormal olarak belirleyebilmektedir (Gökırmak , 2011).

4.7.6. NADIR

NADIR (Network Anomaly Detection and Intrusion Reporter), 1991-1993 yılları arasında Los Alamos Ulusal Laboratuvarları'nda (LANL-Los Alamos National Laboratory) geliştirilmiştir. Yapısında uzman sistemler kullanılan STS, ağda bulunan kullanıcılara yönelik profil analizi yapar ve profilleri haftalık olarak raporlar. Uzman sistemlerde bulunan kurallar ile çıkardığı istatistiği karşılaştırır (Christoph, 1995).

4.7.7. Hyperview

İki bölümden oluşan saldırı tespit sisteminin ilk bölümünde davranışları izleyen ve analiz eden uzman sistemler bulunmaktadır. İkinci bölümünde ise birinci bölümden öğrenilen verilerle eğitim sağlayan YSA (Yapay Sinir Ağları) bulunmaktadır (Axelsson, 2000b).

4.7.8. DIDS

DIDS (Distributed Intrusion Detection System), bir ağdan topladığı verileri analiz eden dağıtık mimarili bir yapıya sahip saldırı tespit sistemidir.

4.7.9. USTAT

1993-1995 yılları arasında Unix (State Transition Analysis Technique for Unix Systems) işletim sistemleri için geliştirilmiştir. USTAT, davranışları durum geçiş analizi yöntemi ile analiz ederek saldırı olup olmadığı tespit etmektedir (Ilgun, 1993; Güven, 2007c)

4.7.10. IDIOT

IDIOT (Intrusion Detection In Our Time) saldırı tespit sistemi, 1994-1996 yılları arasında CERIAS (Center for Education and Research in Information Assurance and Security)'de Kumar tarafından tasarlanmış olup saldırı yöntemlerinin

eşleştirme ve geçici karakteristiklerin karmaşıklığına dayalı olarak tespit eder (Axelsson, 2000c).

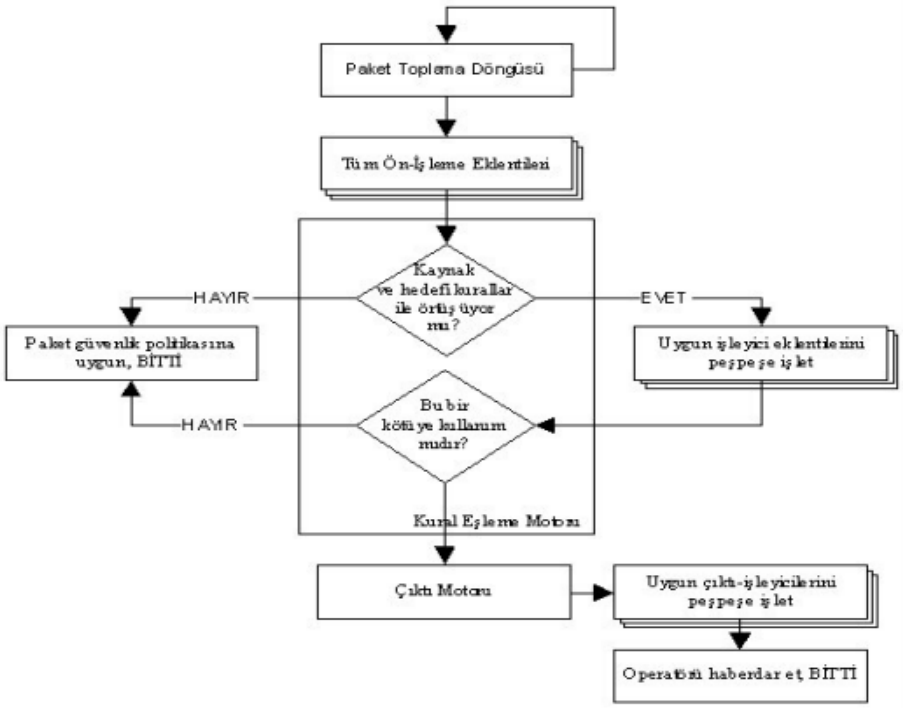
4.7.11. Ripper

1999 yılında geliştirilerek veri madenciliği tekniğini kullanan saldırı tespit sistemidir. DARPA değerlendirmesine katılmıştır (Erol, 2005).

4.7.12. Snort

Snort, daha önceden belirlenmiş olan kuralları temel alarak sisteme gelen giden paketleri analiz eden kural tabanlı bir STS'dir. Snort Lawrence Berkeley National Laboratuarı'nda geliştirilmiş olan libpcap paket yakalama kütüphanesini kullanmaktadır. Libpcap kütüphanesinden faydalanması farklı ağlarda çalışmasına olanak sağlamaktadır.

Snort mimarisine Şekil 4.3'te yer verilmiştir (Dayıoğlu, 2001).



Şekil 4.3 Snort'un mimari yapısı

4.8. STS'lere İlişkin Yapılmış Çalışmalar

Yapay zekanın alt grupları arasında yer alan ve karar verme özelliğine sahip olan makine öğrenmesi metotlarıyla gerçekleştirilen saldırı tespit sistemlerine ilişkin bir çok çalışma bulunmaktadır. Makine öğrenme metotlarının da içerisinde yer aldığı Anomali tabanlı saldırı tespit sistemlerinde öncelikle normal değerlerin tanımı yapılarak akabinde gelen verilerin normal veya anormal olmasına karar vererek sınıflandırma yapabilmektedir. Anormal tabanlı saldırı tespit sistemlerinin imza tabanlı saldırı tespit sistemlerine oranla daha çok tercih edilme sebebi imza tabanlı saldırı tespit sistemlerinin daha önce kaydedilmiş değerlere göre tespit edebilmesi nedeniyle başarı oranı ve tespit süresinin daha düşük olmasıdır. Bu bölümde çalışmada kullanılan makine öğrenme metotları ve bu metotlara yönelik yapılmış çalışmalar ele alınmıştır.

4.8.1. Yapay Sinir Ağları (YSA)

Yapay zekanın alt grupları arasında yer alan Yapay Sinir Ağları, insanın düşünebilme ve öğrenme özelliğini taklit eden akıllı bir algoritmaya dayandırılmaktadır. Tıpkı düşünebilme ve öğrenebilmeyi sağlayan insan beyninde bulunan sinir ağları gibi bir yöntem ile oluşturulmuş tek veya çok katmanlı bir yapılardan oluşmaktadır. Yapay sinir ağlarını meydana getiren 5 parametre bulunmaktadır. Bu parametreler girdiler, ağırlıklar, toplama fonksiyonu, aktivasyon fonksiyonu ve çıktılardır (Öztemel, 2006).

KDD'99 veri seti yapay sinir ağları kullanılarak dos saldırılar (smurf, neptun, back, teardrop), rl2 ve probe saldırılarında en yüksek %97,92 oranında başarı oranı yakalanmıştır. Çalışmada YSA yöntemi sayesinde farklı eğitim ve test kümeleri kullanılarak oldukça düşük hata oranıyla doğru sonuçların elde edildiği görülmüştür (Sağıroğlu vd, 2011).

Murat H. SAZLI ve Haluk TANRIKULU çalışmalarında MATLAB programındaki "Neural Network Tools Box" ile çok katmanlı yapay sinir ağları oluşturarak DARPA veri setlerini eğitmişlerdir. İyi motiflenmiş saldırı tespit sistemiyle Dos

ataklarının oldukça yüksek başarı oranında tespit edilmesini sağlamışlardır (Tanrıkulu ve Sazlı, 2007).

YSA metotlarının STS çalışmalarında tercih edilmesinin nedeni söz konusu metodun yüksek sınıflandırma yapabilme yeteneği, daha önceki öğrenmeden yeni veriler için çıkarım yapabilmesi, eksik bilgi içeren verileri tamamlayabilmesi, yeni olayları öğrenebilmesi gibi bir çok avantaja sahip olmasıdır. Yapay sinir ağını oluşturma kurallarının bulunmaması, çok fazla deneme yapılması nedeniyle öğrenmenin uzun sürmesi ise dezavantajları arasında yer almaktadır.

4.8.2. Naive Bayes Algoritması

Verilerin kategorisine göre sınıflandırma algoritması olan Naif Bayes adını Thomas Bayes'ten (1701 - 7 Nisan 1761) almaktadır. Naïve Bayes algoritması tüm olasılıkları hesaplayarak en yüksek orandaki değeri sınıflandırmaya dahil ettiği için başarı oranı oldukça yüksektir. Kullanılan veriler birden fazla sınıfa sahip ise Multinomial (Çok Terimli) Naive Bayes, verilerde normal bir dağılım söz konusu ise Gauss Naive Bayes, tahminlerin ikili şekilde yapılması isteniyorsa Bernoulli Naive Bayes tercih edilebilmektedir. Hızlı sonuçlanması, yüksek boyutlarda gerçek ve değişkenlik gösteren verilerle çalışılabilmesi gibi avantajlarının yanında değişkenler arasında bulunan ilişkilerin modellenememesi dezavantajları arasında yer almaktadır (Hatipoğlu, 2018).

KDDCup'99 veri seti kullanılarak Naive Bayes algoritmasıyla gerçekleştirilen saldırı tespit sistemi çalışmasında %95 başarı oranıyla 1.89 saniyede saldırıları tespit eden sistem gerçekleştirilmiş olup KNN (K-means clustering algorithm) ve YSA metotlarından daha iyi olduğu gösterilmiştir. (Panda, 2007).

Shital K. Ajagekar ve Vaishali Jadhav'ın Web üzerindeki DDOS atakların Multinomial NB algoritmasıyla sınıflandırılarak %79 - %99,5 aralığında tespit edilmesi sağlanmış ve en yüksek oranda başarı HTTP-flooding atağının tespitinde yakalanmıştır (Ajagekar, 2016).

4.8.3. K En Yakın Komşu Algoritması (KNN)

Verilerin sahip olduğu özniteliklerin sınıflandırılma aşamasında yeni özniteliğin önceki k tane özniteliğe yakınlığını hesaplayan algoritmadır. NSL-KDD veri setiyle farklı öznitelikler seçilerek kNN-1, kNN-2, J-48, Naif Bayes algoritmaları denenmiştir. En yüksek başarı oranın PCA 21 nitelikli ve orijinal veri seti üzerinde kNN-1 ve J-48 algoritmaları ile elde edildiği görülmektedir (Çavuşoğlu ve Kaçar, 2019).

4.8.4. Karar Ağacı (Decison Tree) Algoritması

Karar Ağacı algoritması kullanılarak gerçekleştirilen sınıflandırma yöntemi karar düğümleri, yapraklar ve dallardan oluşmaktadır. Sınıflandırılmanın gerçekleşip gerçekleşmemesine bağlı olarak yapraklar veya karar düğümleri meydana gelir. CICIDS2017 veri seti kullanılarak gerçekleştirilen çalışmada %99 gibi oldukça yüksek başarı oranında karar ağacı algoritması kullanılarak saldırı tespiti gerçekleştirilmiştir. Veri setinde bulunan Hizmet Engelleme (Dos), Dağıtılmış Hizmet Reddi (DDoS) ve Port Tarama (PortScan) saldırılarının anormal olarak nitelendirildiği ve tespit etmek için 78 adet trafik özelliği kullanıldığı görülmüştür (Özekes ve Karakoç, 2019).

4.8.5. Rasgele Orman (Random Forest) Sınıflandırma Algoritması

Rastgele orman sınıflandırıcısı, seçilen eğitimin ve değişkenlerin alt kümesini kullanarak çoklu karar ağaçları üreten bir topluluk sınıflandırıcısıdır (Belgiu ve Draguţ, 2016). CSE-CIC-IDS2018 veri seti kullanılarak gerçekleştirilen LGBM, CNN ve Rastgele Orman yöntemleri denenmiş olup Rasgele Orman Modeliyle oluşturulmuş iki seviyeli hibrit yapının 0.86 F-skor macro ortalaması ile en yüksek başarıma sahip olduğu görülmüştür (Pehlivanoğlu vd., 2019).

4.8.6. Destek Vektör Makineleri (DVM-SVM)

Destek Vektör Makineleri Algoritması temel olarak iki sınıfı en iyi şekilde birbirinden ayırt etmek için kullanılan bir algoritmadır. Wani ve arkadaşları 2019 yılındaki çalışmalarında SVM, Rastgele Orman ve Naive Bayes yöntemlerini kullanarak Bulut Bilişim Ortamı üzerinde DDoS saldırıları tespiti yapmışlardır. Çalışma hususunda oluşturulan veri kümesi içerisinden 9 öznitelik kullanılarak en başarılı sonuç 0.998 F-skoru ile SVM algoritmasından alınmıştır (Wani vd., 2019).

5 VERİ SETİ VE UYGULAMA

5.1. Veri Seti

Saldırı Tespit Sistemi tasarımlarında farklı algoritmalar uygulanarak yapılan çalışmalarda birçok veri seti kullanılmaktadır. Kanada Siber Güvenlik Enstitüsü tarafından paylaşılan, uygun bir test ortamında hazırlanmış CICDDoS2019 veri seti daha önceki Enstitünün hazırlamış olduğu veri setlerindeki eksiklikler göz önüne alınarak tasarlanmış en güncel veri setidir. (UNB, 2019) CICDDoS2019, gerçek verilere (PCAP'ler) benzeyen iyi huylu ve en güncel DDoS saldırılarıyla birlikte zaman damgası, kaynak ve hedef IP'lere, kaynak ve hedef bağlantı noktalarına, protokollere ve saldırıya (CSV dosyaları) dayalı etiketli akışlara sahip CICFlowMeter-V3 kullanan ağ trafiği analizinin sonuçlarını da içermektedir. Bu veri kümesinde PortMap, NetBIOS, LDAP, MSSQL, UDP, UDP-Lag, SYN, NTP, DNS ve SNMP gibi farklı DDoS saldırı çeşitleri mevcuttur (UNB, 2019).

5.1.1. Veri seti kullanılarak yapılan çalışmalar

CICDDoS2019 veri setinin üretilerek ilk yapılan çalışma veri setinde bulunan her bir DDoS saldırılarından 80 özellikten en iyi algılama özelliğini seçmek için, çıkarılan özellikler Random Forest Regressor kullanarak test edilmiştir. Çalışmanın amacı oluşturulan yeni veri setiyle 11 çeşit DDOS saldırısı incelenerek tespit edilebilmesi için en iyi özniteliklerin çıkarılması sağlanmıştır (Sharafaldin ve Friends, 2019).

5.2. Uygulama

Bu çalışmada CICDDoS2019 veri seti kullanılarak 83 öz niteliğe sahip DDOS saldırısı olan ve iyi huylu (benign) değerler incelenmiştir. Veri seti içerisinde bulunan boşluk, string, port numaraları gibi birçok değer kullanılabilir olmadığı için C ve C++ programlarıyla ön işlemeye tabii tutularak çıkarılmış ve eğitilebilir duruma getirilmiştir. Veri setinde bulunan 83 öz nitelik içerisinden eğitime tabi

tutulacak 76 öz nitelik ve 1 adet saldırı olup olmadığını değerlendiren etiket ile 77 öz nitelik olacak şekilde eğitime hazır veri seti oluşturulmuştur.

Veri Seti içerisinde DDOS atağına ve zararsız verilere ait toplam 3 milyon ön işlemden geçmiş veri bulunmaktadır. Söz konusu veri seti baz alınarak Brute Force yöntemiyle seçilmiş toplam 50'şer adet 4'lü, 8'li, 10'lu ve 12'li öz nitelik değerlere sahip veri setleri oluşturulmuştur. Söz konusu öz nitelik değerleri ilk olarak Pyhon Pycharm programında oluşturulan Yapay Sinir Ağları yöntemiyle eğitime tabii tutulmuştur.

Ortaya çıkan sonuçlar arasında en iyi öznitelikler ve başarı oranlarına Çizelge 5.1'de yer verilmiştir. Özelliklere ve başarı oranlarına bakıldığında ise en yüksek başarı oranı oranıyla en kısa sürede DDOS atağının tespiti 4 adet özelliğin bulunduğu değerler ile gerçekleştirilmiştir.

Çizelge 5.1 YSA yöntemiyle DDOS saldırısı tespiti için en iyi özellikler

Özellik	**Açıklama**
4'lü Özellik ile En iyi Değerler (Başarı oranı: %0,993)	
Tot Fwd Pkts	İleri yönde toplam paket sayısı
Tot Len Bwd Pkts	Geri yönde paketlerin toplam uzunluğu
Bwd IAT Mean	Geri yönde gönderilen iki paket arasındaki ortalama zaman
Fwd Seg Size Min	İleri yönde gözlenen minimum boyut
6'lı Özellik ile En iyi Değerler (Başarı oranı: % 0,994)	
Bwd Pkt Len Std	Geri yönde paket uzunluklarının standart sapması
Flow IAT Max	Paketlerin maximum varış zamanı
Pkt Len Min	Bir akışın minimum uzunluğu
Down/Up Ratio	İndirme ve yükleme oranı
Fwd Byts/b Avg	İleri yönde iletilen ortalama byte sayısı
Fwd Seg Size Min	İleri yönde gözlenen minimum boyut
8'li Özellik ile En iyi Değerler (Başarı oranı: 0,973)	
Bwd Pkt Len Max	Geri yönde paketlerin maksimum uzunluğu
Flow IAT Std	Paketlerin varış zamanlarının standart sapması
Flow IAT Min	Paketlerin Minimum varış zamanı

Fwd IAT Tot	İleri yönde gönderilen iki paket arasındaki toplam zaman
Bwd IAT Std	Geri yönde gönderilen iki paket arasındaki zamanın standart sapması
Fwd Pkts/s	Saniyedeki ileri yön paket sayısı
Pkt Len Std	Bir akışın standart sapması
SYN Flag Cnt	SYN içeren paket sayısı
10'lu Özellik ile En iyi Değerler (Başarı oranı: 0,979)	
Fwd Pkt Len Mean	İleri yönde paketlerin ortalama uzunluğu
Bwd Pkt Len Min	İleri yönde paketlerin minimum uzunluğu
Bwd Pkt Len Mean	Geri yönde paketlerin ortalama uzunluğu
Fwd IAT Max	İleri yönde gönderilen iki paket arasındaki maksimum zaman
Bwd PSH Flags	Geri yönde hareket eden paketlerde PSH bayrağının aktif olma sayısı (UDP için 0)
Fwd Pkts/s	Saniyedeki ileri yön paket sayısı
FIN Flag Cnt	FIN içeren paket sayısı
SYN Flag Cnt	SYN içeren paket sayısı
PSH Flag Cnt	PUSH içeren paket sayısı
Down/Up Ratio	İndirme ve yükleme oranı
12'li Özellik ile En iyi Değerler (Başarı oranı: 0,998)	
Bwd Pkt Len Min	Geri yönde paketlerin minimum uzunluğu
Flow Pkts/s	**Saniyede akan paket sayısı**
Flow IAT Min	Paketlerin minimum varış zamanı
Fwd IAT Tot	İleri yönde gönderilen iki paket arasındaki toplam zaman
Bwd IAT Std	Geri yönde gönderilen iki paket arasındaki zamanın standart sapması
Fwd URG Flags	İleri yönde hareket eden paketlerde URG bayrağının aktif olma sayısı (UDP için 0)
Fwd Header Len	İleri yöndeki başlıklar için kullanılan toplam byte
Bwd Header Len	Geri yöndeki başlıklar için kullanılan toplam byte
Bwd Pkts/s	Saniyedeki geri yön paket sayısı
Subflow Bwd Pkts	Geri yönde bir alt akıştaki ortalama paket sayısı
Fwd Act Data Pkts	TCP veri taşıma kapasitesinin en az 1 bayt içeren paket sayısı
Fwd Seg Size Min	İleri yönde gözlenen minimum boyut

4, 6, 8, 10 ve 12'şerli özelliğe sahip her biri 500 bin adet olan veri setleri oluşturularak Gaussian Naïve Bayes, Multinomial Naive Bayes, Bernoulli Naive Bayes, Logistic Regresyon, K-nearest neighbour (KNN), Decision Tree (entropy-gini), Random Forest ve SVM algoritmalarıyla eğitilmiştir. Eğitim sonucunda DDOS atağı en yüksek oranda ve en kısa sürede tespit eden özelliklere Çizelge 5.2'de yer verilmiştir.

Çizelge 5.2 DDOS saldırısı tespiti için kullanılan algoritmalar, başarı oranları

Eğitim için kullanılan algoritma	Başarı Oranı (%)	Tespit Süresi (sn)
Logistic Regrasyon	99,8	788
Gaussian Naive Bayes	98,7	1041
k-nearest neighbor	99,9	1040
Multinomial Naive Bayes	99,1	1041
Bernoulli Naive Bayes	99,8	1042
Decision Tree(entropy)	99,12	1043
Decision Tree(gini)	99,34	1043
Random Forest	98,4	1047
SVM	99,7	1074

Kullanılan veri setinin %70'i eğitim ve %30'u test için ayrılmıştır. Çizelge 5.2'de yer alan algoritmalar ile eğitim gerçekleştirildiğinde en yüksek başarı oranına sahip özelliklere aşağıdaki Çizelge 5.3'te yer verilmiştir.

Çizelge 5.3 En yüksek başarı oranına sahip özellikleri içeren veri seti

Özellik	Açıklama
Tot Bwd Pkts	Geri yönde toplam paket sayısı
Fwd Pkt Len Min	İleri yönde paketlerin minimum uzunluğu
Bwd Pkt Len Min	Geri yönde paketlerin minimum uzunluğu
Bwd Pkt Len Mean	Geri yönde paketlerin ortalama uzunluğu
Flow Byts/s	Saniyede akan byte sayısı
Flow Pkts/s	Saniyede akan paket sayısı
Flow IAT Std	Paketlerin varış zamanlarının standart sapması
Bwd IAT Mean	Geri yönde gönderilen iki

	paket arasındaki ortalama zaman
Fwd Header Len	İleri yöndeki başlıklar için kullanılan toplam byte
Pkt Len Std	Bir akışın standart sapması
Pkt Len Var	Bir akışın uzunluk varyansı
CWE Flag Count	CWE içeren paket sayısı

Çizelge 5.4 Dört adet özelliğe sahip veri setindeki tehdide ait özellikler

Özellik	mean	std	min	25%	50%	75%	max
Tot Fwd Pkts	106	3549	0	1	2	5	309628
Tot Len Bwd Pkts	3366	239305	0	0	0	508	101000000
Bwd IAT Mean	593222	4045617	0	0	0	25736	120000000
Fwd Seg Size Min	10	12	0	0	0	20	44

Çizelge 5.5 Dört adet özelliğe sahip veri setindeki tehdide ait özellikler

Özellik	mean	std	min	25%	50%	75%	max
Tot Fwd Pkts	205	5017	0	1	1	1	309628
Tot Len Bwd Pkts	1128	120350	0	0	0	0	40921490
Bwd IAT Mean	536821	4928832	0	0	0	0	117120000
Fwd Seg Size Min	0	0	0	0	0	0	0

Çizelge 5.6 Dört adet özelliğe sahip veri setindeki tehdit olmayan özellikler

Özellik	mean	std	min	25%	50%	75%	max
Tot Fwd Pkts	7	91	1	2	5	8	43159
Tot Len Bwd Pkts	5605	316290	0	51	316	978	101000000
Bwd IAT Mean	649622	2904188	0	0	16912	259979	120000000

Fwd Seg Size Min	20	8	0	20	20	20	44

Çizelge 5.7 Altı adet özelliğe sahip veri setindeki tehdide ait özellikler

Özellik	mean	std	min	25%	50%	75%	max
Bwd Pkt Len Std	130	191	0	0	0	216	2780
Flow IAT Max	4717421	15475910	0	1661	13891	1134714	120000000
Pkt Len Min	4	15	0	0	0	0	1232
Down/Up Ratio	1	1	0	0	1	1	148
Fwd Byts/b Avg	0	0	0	0	0	0	0
Fwd Seg Size Min	10	12	0	0	0	20	44

Çizelge 5.8 Altı adet özelliğe sahip veri setindeki tehdide ait özellikler

Özellik	mean	std	min	25%	50%	75%	max
Bwd Pkt Len Std	90	183	0	0	0	0	2780
Flow IAT Max	1543225	9121830	0	1704	5463	15333	119978100
Pkt Len Min	0	1	0	0	0	0	301
Down/Up Ratio	1	0	0	1	1	1	7
Fwd Byts/b Avg	0	0	0	0	0	0	0
Fwd Seg Size Min	0	0	0	0	0	0	0

Çizelge 5.9 Altı adet özelliğe sahip veri setindeki tehdit olmayan özellikler

Özellik	mean	std	min	25%	50%	75%	max
Bwd Pkt Len Std	170	190	0	0	164	244	1243
Flow IAT Max	7891618	19381660	1	1279	953167	4370986	120000000
Pkt Len Min	9	20	0	0	0	0	1232
Down/Up Ratio	0	1	0	0	0	1	148
Fwd Byts/b Avg	0	0	0	0	0	0	0
Fwd Seg Size Min	20	8	0	20	20	20	44

Çizelge 5.10 Sekiz adet özelliğe sahip veri setindeki tehdide ait özellikler

Özellik	mean	std	min	25%	50%	75%	max
Fwd Pkt Len Mean	59	76	0	0	19	134	1460
Bwd Pkt Len Min	10	36	0	0	0	0	1448
Flow IAT Min	2225537	12530340	0	6	291	3244	120000000
,Fwd IAT Mean	2635965	12434190	0	0	83	316183	120000000
Bwd IAT Std	673210	4098803	0	0	0	16648	84800000
Bwd URG Flags	0	0	0	0	0	0	20
Fwd Pkts/s	9188	117818	0	2	86	604	3000000
CWE Flag Count	0	0	0	0	0	0	1

Çizelge 5.11 Sekiz adet özelliğe sahip veri setindeki tehdide ait özellikler

Özellik	mean	Std	min	25%	50%	75%	max
Fwd Pkt Len Mean	31	63	0	0	0	0	933
Bwd Pkt Len Min	0	14	0	0	0	0	1448
Flow IAT Min	313460	3447488	0	489	1887	8588	119978100
Fwd IAT Mean	220448	1616836	0	0	0	0	118246400
Bwd IAT Std	530361	4645713	0	0	0	0	84474020
Bwd URG Flags	0	0	0	0	0	0	20
Fwd Pkts/s	758	7298	0	67	209	585	1000000
CWE Flag Count	0	0	0	0	0	0	1

Çizelge 5.12 Sekiz adet özelliğe sahip veri setindeki tehdit olmayan özellikler

Özellik	mean	Std	min	25%	50%	75%	max
Fwd Pkt Len Mean	87	77	0	26	54	178	1460
Bwd Pkt Len Min	20	46	0	0	0	0	1430
Flow IAT Min	4137614	17170370	0	5	29	281	120000000
Fwd IAT Mean	5051482	17173660	0	125	277972	1111055	120000000
Bwd IAT Std	816060	3460770	0	0	5710	293210	84800000
Bwd URG Flags	0	0	0	0	0	0	0
Fwd Pkts/s	17618	166033	0	1	4	827	3000000
CWE Flag Count	0	0	0	0	0	0	0

Çizelge 5.13 On adet özelliğe sahip veri setindeki tehdide ait özellikler

Özellik	mean	std	min	25%	50%	75%	max
Tot Bwd Pkts	5	166	0	1	1	4	69196
Bwd Pkt Len Min	10	36	0	0	0	0	1448
Fwd IAT Std	867981	3256981	0	0	0	355524	84200000
Fwd IAT Min	2133883	12432830	0	0	3	143	120000000
Bwd IAT Mean	595803	4070240	0	0	0	25627	120000000
Bwd IAT Min	131666	2817564	0	0	0	207	120000000
URG Flag Cnt	0	0	0	0	0	0	1
Down/Up Ratio	1	1	0	0	1	1	115
Fwd Seg Size Avg	59	75	0	0	19	134	1460
Bwd Seg Size Avg	89	147	0	0	0	139	2073

Çizelge 5.14 On adet özelliğe sahip veri setindeki tehdide ait özellikler

Özellik	mean	std	min	25%	50%	75%	max
Tot Bwd Pkts	3	86	1	1	1	1	29481
Bwd Pkt Len Min	0	13	0	0	0	0	1448
Fwd IAT Std	296600	2295999	0	0	0	0	70701950
Fwd IAT Min	19747	517086	0	0	0	0	118246400
Bwd IAT Mean	542053	4968693	0	0	0	0	117120000
Bwd IAT Min	129272	3388424	0	0	0	0	117120000
URG Flag Cnt	0	0	0	0	0	0	0
Down/Up Ratio	1	0	0	1	1	1	7
Fwd Seg Size Avg	31	63	0	0	0	0	933
Bwd Seg	47	118	0	0	0	0	2073

Size Avg							

Çizelge 5.15 On adet özelliğe sahip veri setindeki tehdit olmayan özellikler

Özellik	mean	std	min	25%	50%	75%	max
Tot Bwd Pkts	8	218	0	1	3	7	69196
Bwd Pkt Len Min	20	46	0	0	0	0	1232
Fwd IAT Std	1439158	3910211	0	0	148266	2041703	84200000
Fwd IAT Min	4247264	17317450	0	3	34	225	120000000
Bwd IAT Mean	649535	2905674	0	0	16776	259918	120000000
Bwd IAT Min	134058	2096946	0	0	39	15888	120000000
URG Flag Cnt	0	0	0	0	0	0	1
Down/Up Ratio	0	1	0	0	0	1	115
Fwd Seg Size Avg	87	77	0	26	54	171	1460
Bwd Seg Size Avg	131	161	0	43	109	183	1956

Çizelge 5.16 Oniki adet özelliğe sahip veri setindeki tehdide ait özellikler

Özellik	mean	std	min	25%	50%	75%	max
Bwd Pkt Len Min	10	35	0	0	0	0	1448
Flow Pkts/s	11739	127066	0	5	192	1244	3000000
Flow IAT Min	2209051	12479380	0	6	290	3233	1,2E+08
Fwd IAT Tot	7300558	23594600	0	0	85	2433093	1,2E+08
Bwd IAT Std	671775	4086683	0	0	0	16863	84500000
Fwd URG Flags	0	0	0	0	0	0	0
Fwd Header	917	28632	0	20	32	152	2178688

Len							
Bwd Header Len	112	2943	0	20	20	124	1377272
Bwd Pkts/s	2557	36285	0	1	64	552	2000000
Subflow Bwd Pkts	5	148	0	1	1	5	68863
Fwd Act Data Pkts	104	3565	0	0	0	1	272336
Fwd Seg Size Min	10	12	0	0	0	20	40

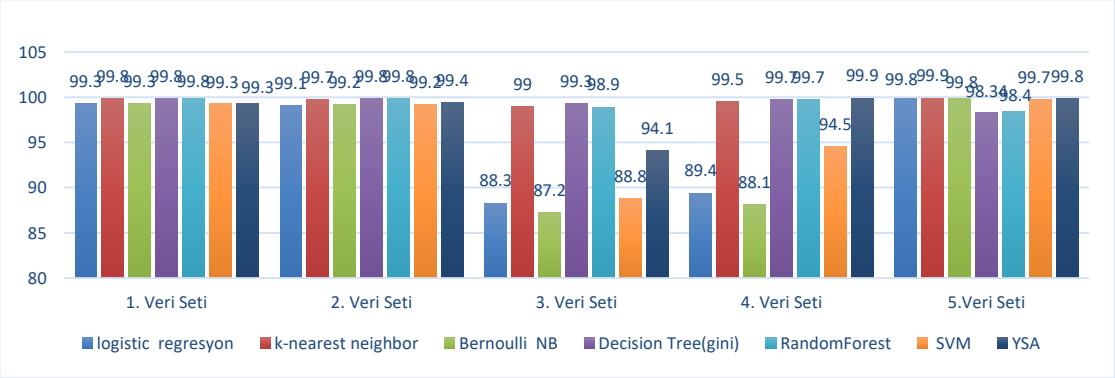
Çizelge 5.17 Oniki adet özelliğe sahip veri setindeki tehdide ait özellikler

Özellik	**mean**	**std**	**min**	**25%**	**50%**	**75%**	**max**
Bwd Pkt Len Min	0	13	0	0	0	0	1448
Flow Pkts/s	3406	35981	0	139	543	1206	2000000
Flow IAT Min	312941	3437693	0	492	1887	8572	119978100
Fwd IAT Tot	1541083	11148870	0	0	0	0	120000000
Bwd IAT Std	528425	4628617	0	0	0	0	84474020
Fwd URG Flags	0	0	0	0	0	0	0
Fwd Header Len	1682	40327	0	20	20	32	2178688
Bwd Header Len	60	1762	0	20	20	32	589620
Bwd Pkts/s	2662	33925	0	69	324	631	2000000
Subflow Bwd Pkts	3	88	0	1	1	1	29481
Fwd Act Data Pkts	206	5040	0	0	0	0	272336
Fwd Seg Size Min	0	0	0	0	0	0	0

Çizelge 5.18 Oniki adet özelliğe sahip veri setindeki tehdit olmayan özellikler

Özellik	mean	std	min	25%	50%	75%	max
Bwd Pkt Len Min	10	35	0	0	0	0	1448
Flow Pkts/s	11739	127066	0	5	192	1244	3000000
Flow IAT Min	2209051	12479380	0	6	290	3233	1,2E+08
Fwd IAT Tot	7300558	23594600	0	0	85	2433093	1,2E+08
Bwd IAT Std	671775	4086683	0	0	0	16863	84500000
Fwd URG Flags	0	0	0	0	0	0	0
Fwd Header Len	917	28632	0	20	32	152	2178688
Bwd Header Len	112	2943	0	20	20	124	1377272
Bwd Pkts/s	2557	36285	0	1	64	552	2000000
Subflow Bwd Pkts	5	148	0	1	1	5	68863
Fwd Act Data Pkts	104	3565	0	0	0	1	272336
Fwd Seg Size Min	10	12	0	0	0	20	40

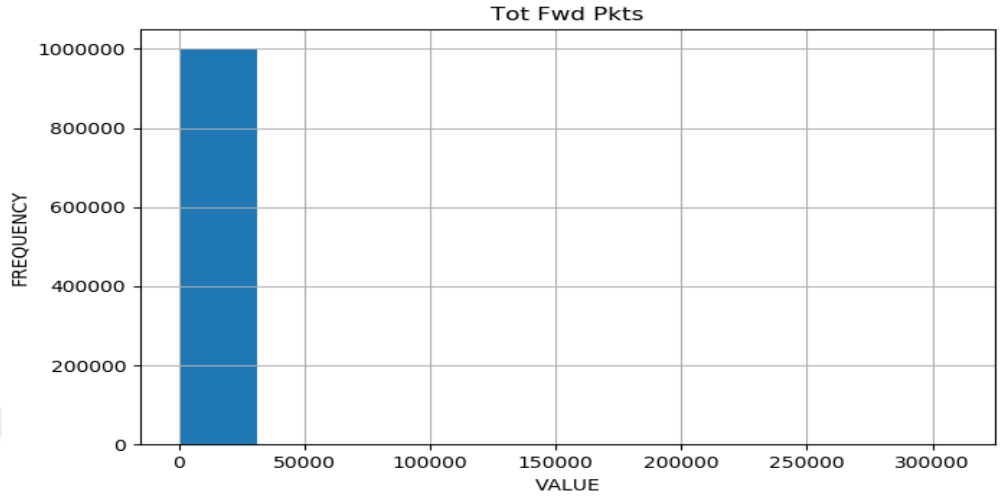
Şekil 5.1'de yer alan grafikte eğitim sonunda en yüksek başarı oranında tespitin gerçekleştiği algoritmalara ve veri setlerine yer verilmiştir.



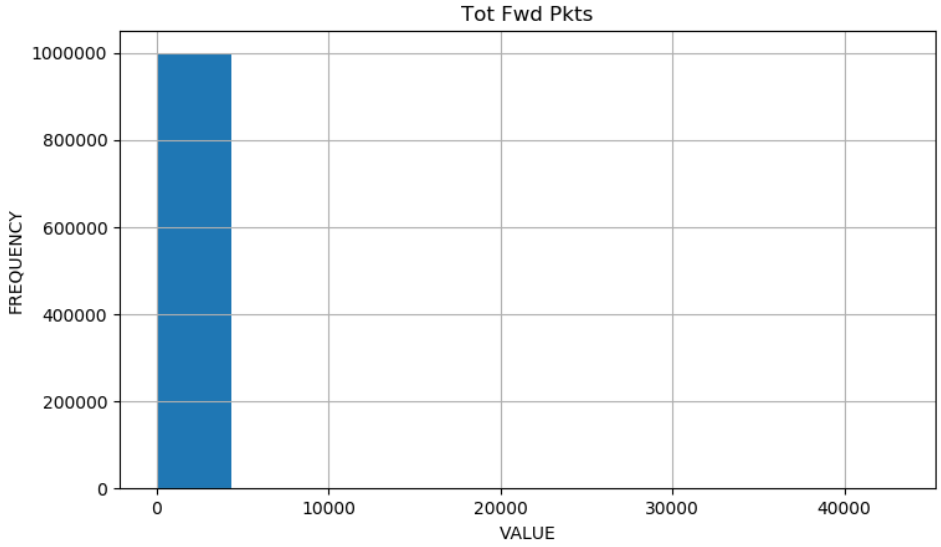
Şekil 5.1 Algoritmaların doğruluk oranlarının karşılaştırılması

Birinci Veri seti olan 4 adet özellik ve etiket değerinden oluşan veri setinde DDOS saldırının tespitinde en belirleyici özelliğin veri analiz edildiğinde Şekil 5-2 ve Şekil 5-3'teki Tot Fwd Pkts özelliği olduğu görülmektedir. Veri setinde yer

alan tehdit durumu ve tehdit olmayan örnekler incelendiğinde farklı değerlerde ve farklı frekanslarda oldukları, veri setlerinde hangi değerlerin bulunduğunu ve kaçının aynı değerden olduğunu gösterir.



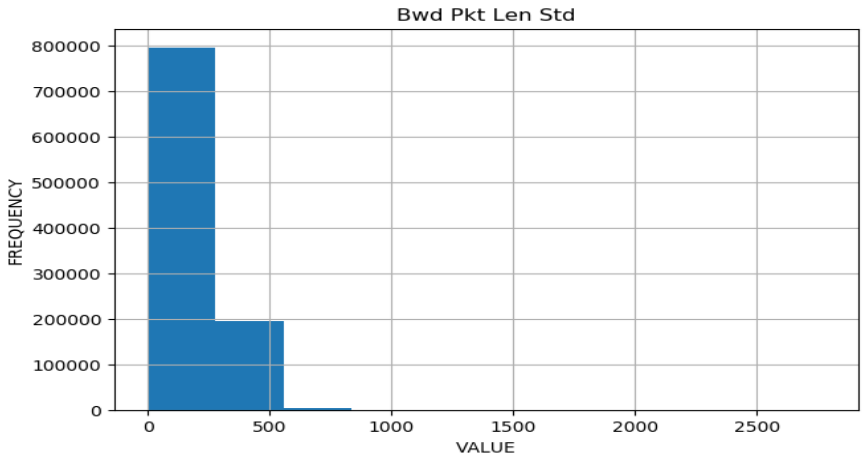
Şekil 5.2 1.veri setinde yer alan en iyi özelliğe ilişkin grafik



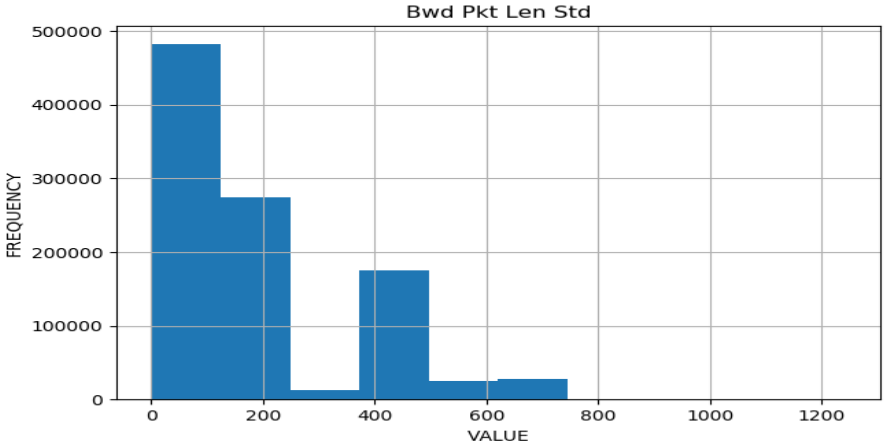
Şekil 5.3 1.veri setinde yer alan en iyi özelliğe ilişkin grafik

2. veri olan 6 adet özellik ve etiket değerinden oluşan veri setinde DDOS saldırının tespitinde en belirleyici özelliklerin veri analiz edildiğinde Şekil 5-4, Şekil 5-5, Şekil 5-6 ve Şekil 5-7'deki Fwd Seg Size Min ve Bwd Pkt Len Std özellikleri olduğu görülmektedir. . Veri setinde yer alan tehdit durumu ve tehdit

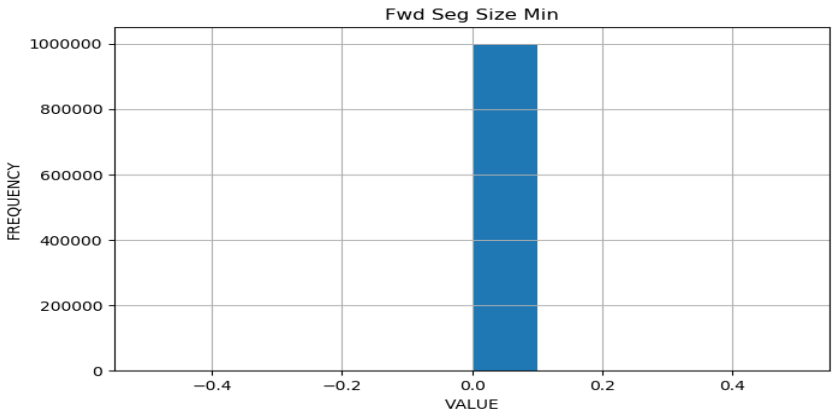
olmayan örnekler incelendiğinde farklı değerlerde ve farklı frekanslarda oldukları, veri setlerinde hangi değerlerin bulunduğunu ve kaçının aynı değerden olduğunu gösterir.



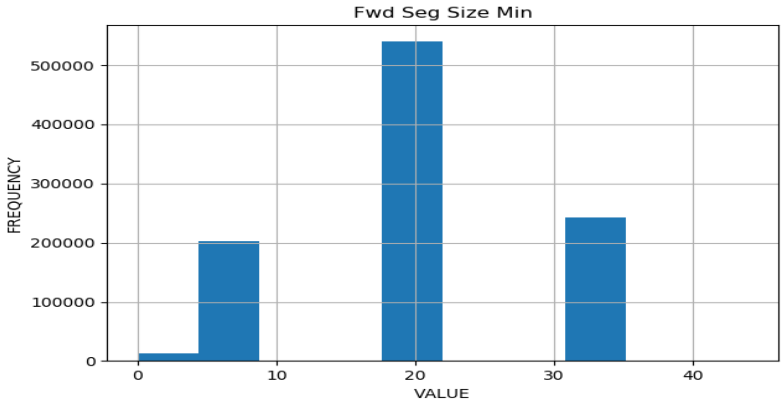
Şekil 5.4 2.veri setinde yer alan en iyi özelliğe ilişkin grafik



Şekil 5.5 2.veri setinde yer alan en iyi özelliklere ilişkin grafik

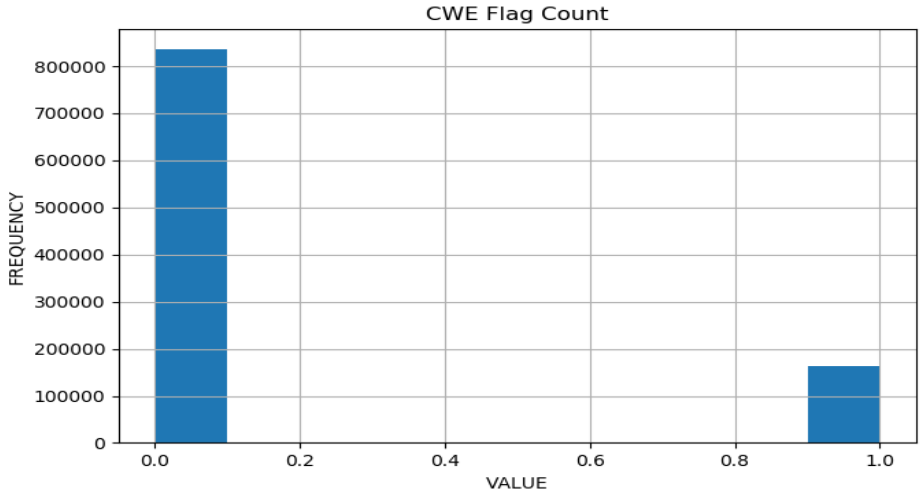


Şekil 5.6 2.veri setinde yer alan en iyi özelliğe ilişkin grafik

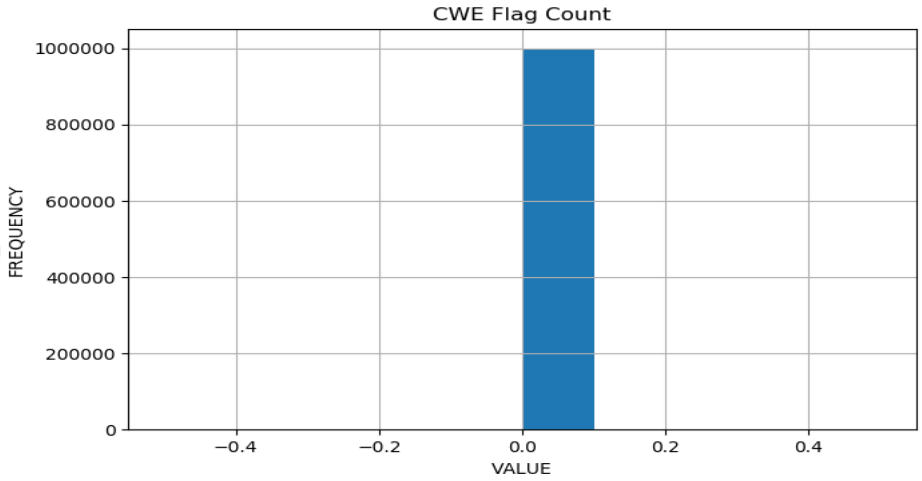


Şekil 5.7 2.veri setinde yer alan en iyi özelliğe ilişkin grafik

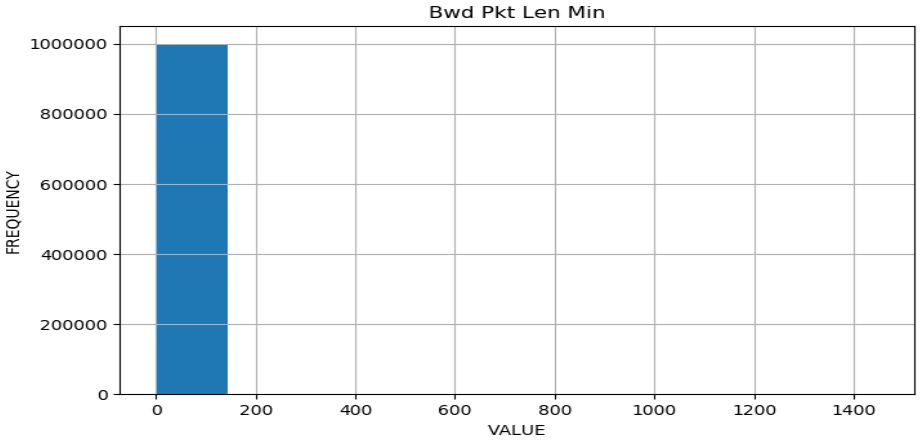
3. veri seti olan 8 adet özellik ve etiket değerinden oluşan veri setinde DDOS saldırının tespitinde en belirleyici özelliklerin veri analiz edildiğinde Şekil 5.8, Şekil 5.9, Şekil 5.10, Şekil 5.11'deki Fwd Pkt Len Min ve CWE Flag Count özellikleri olduğu görülmektedir. Veri setinde yer alan tehdit durumu ve tehdit olmayan örnekler incelendiğinde farklı değerlerde ve farklı frekanslarda oldukları, veri setlerinde hangi değerlerin bulunduğunu ve kaçının aynı değerden olduğunu gösterir.



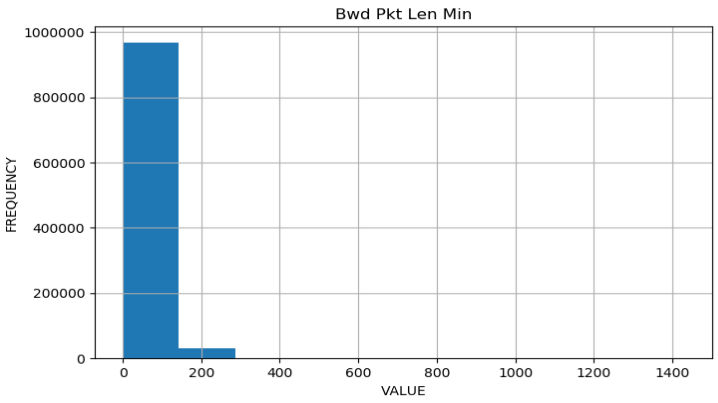
Şekil 5.8 3.veri setinde yer alan en iyi özelliğe ilişkin grafik



Şekil 5.9 3.veri setinde yer alan en iyi özelliğe ilişkin grafik

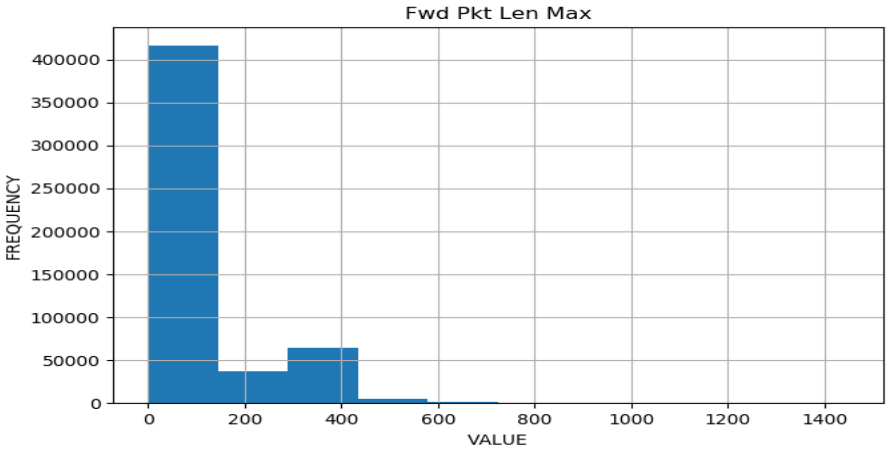


Şekil 5.10 3.veri setinde yer alan en iyi özelliğe ilişkin grafik

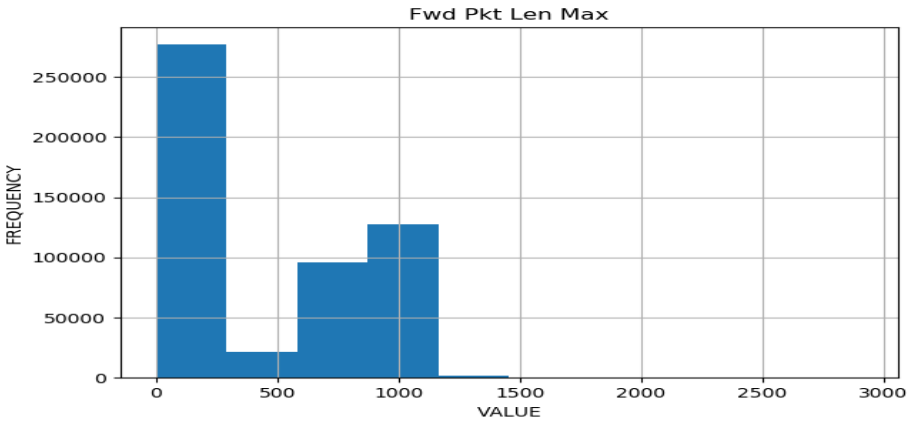


Şekil 5.11 3.veri setinde yer alan en iyi özelliğe ilişkin grafik

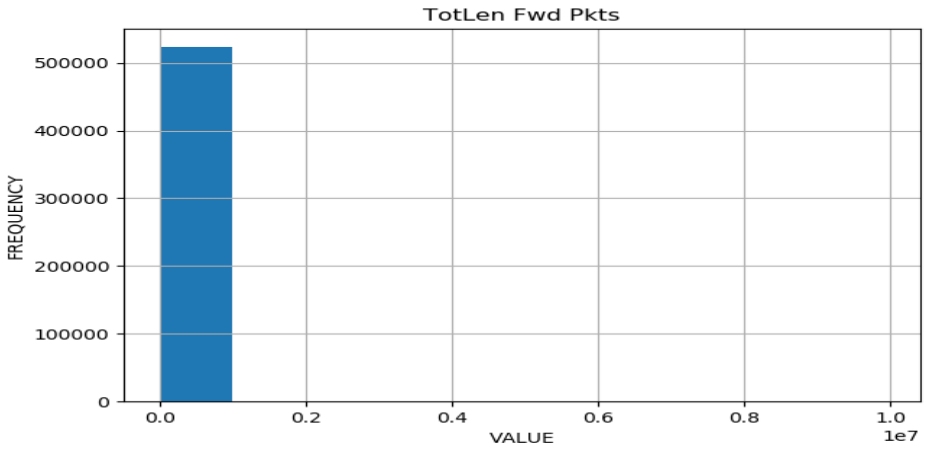
4. veri seti olan 10 adet özellik ve etiket değerinden oluşan veri setinde DDOS saldırının tespitinde en belirleyici özelliklerin veri analiz edildiğinde Şekil 12, Şekil 13, Şekil 14, Şekil 15'deki Fwd Pkt Len Max ve Tot Len Fwd Pkts özellikleri olduğu görülmektedir. Veri setinde yer alan tehdit durumu ve tehdit olmayan örnekler incelendiğinde farklı değerlerde ve farklı frekanslarda oldukları, veri setlerinde hangi değerlerin bulunduğunu ve kaçının aynı değerden olduğunu gösterir.



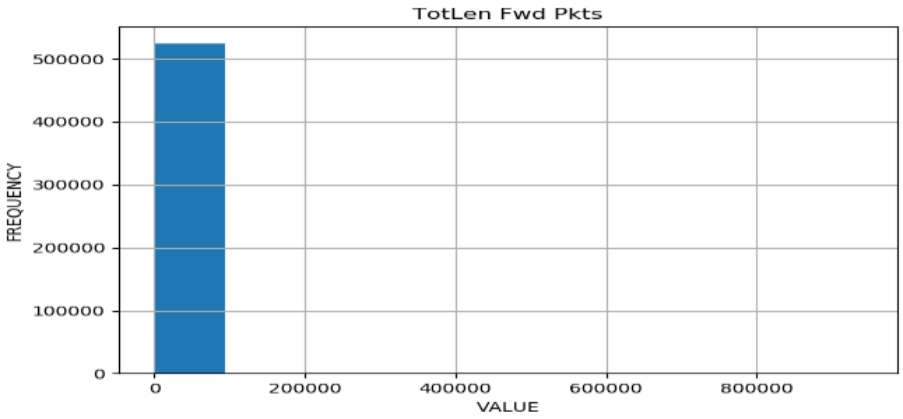
Şekil 5.12 4.veri setinde yer alan en iyi özelliğe ilişkin grafik



Şekil 5.13 4.veri setinde yer alan en iyi özelliğe ilişkin grafik

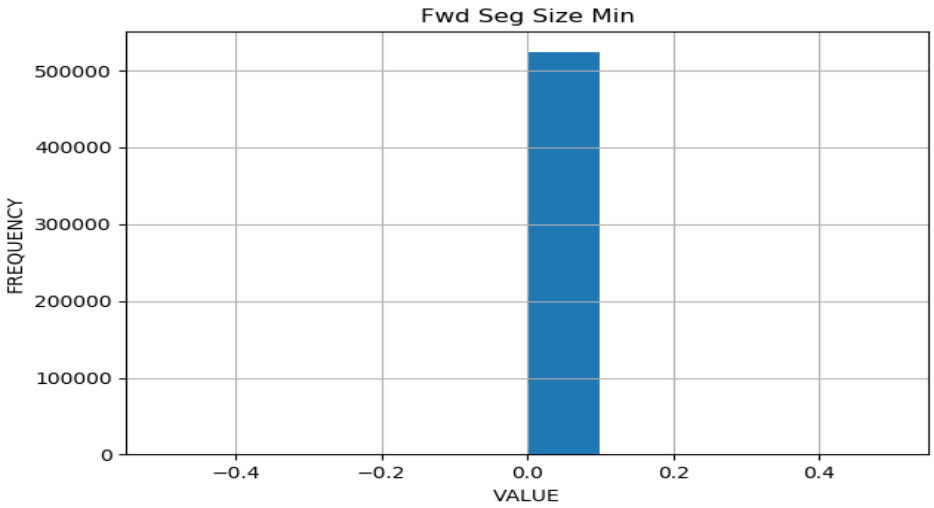


Şekil 5.14 4.veri setinde yer alan en iyi özelliğe ilişkin grafik

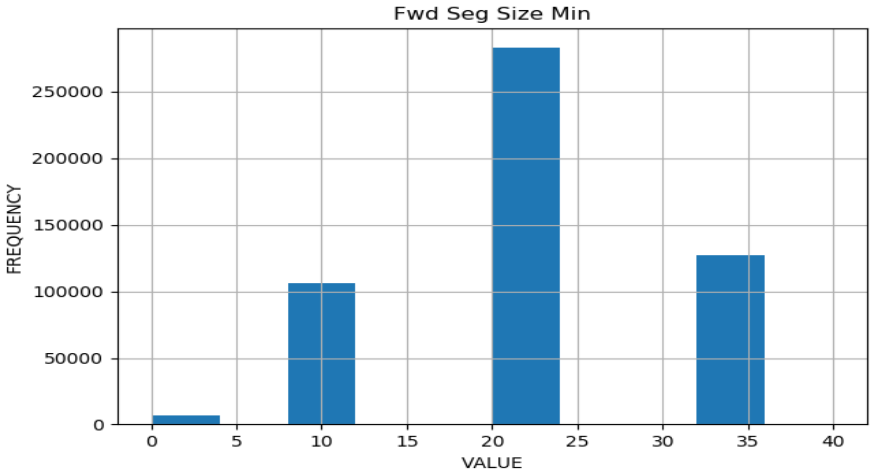


Şekil 5.15 4.veri setinde yer alan en iyi özelliğe ilişkin grafik

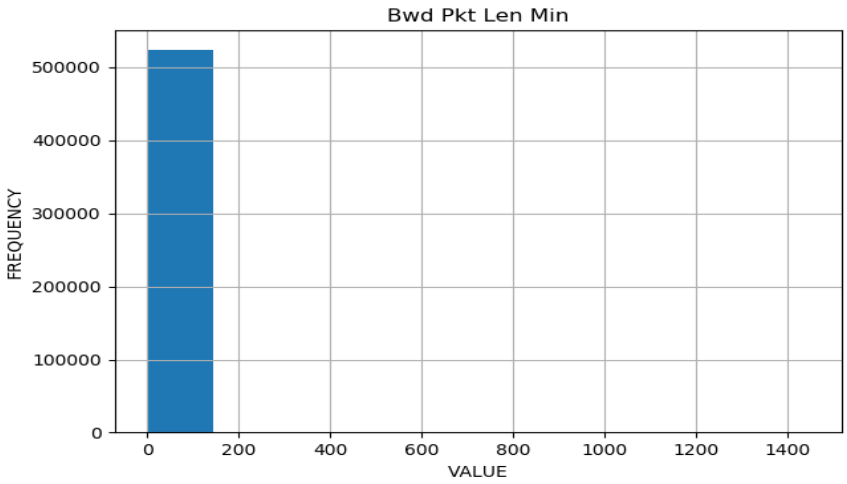
5. veri seti olan 12 adet özellik ve etiket değerinden oluşan veri setinde DDOS saldırının tespitinde en belirleyici özelliklerin veri analiz edildiğinde Şekil 16, Şekil 17, Şekil 18 ve Şekil 19'daki Fwd Seg Size Min ve Bwd Pkt Len Min özellikleri olduğu görülmektedir. Veri setinde yer alan tehdit durumu ve tehdit olmayan örnekler incelendiğinde farklı değerlerde ve farklı frekanslarda oldukları, veri setlerinde hangi değerlerin bulunduğunu ve kaçının aynı değerden olduğunu gösterir.



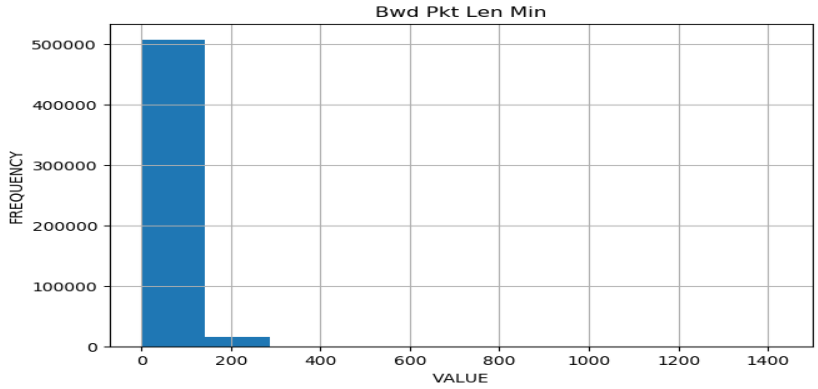
Şekil 5.16 5.veri setinde yer alan en iyi özelliğe ilişkin grafik



Şekil 5.17 5.veri setinde yer alan en iyi özelliğe ilişkin grafik



Şekil 5.18 5.veri setinde yer alan en iyi özelliğe ilişkin grafik



Şekil 5.19 5.veri setinde yer alan en iyi özelliğe ilişkin grafik

6. SONUÇ VE ÖNERİLER

Tez çalışması kapsamında bilgi güvenliğine yönelik saldırıların yüksek doğruluk oranı ve kısa sürede tespit edilmisini sağlayan STS'lerde güncel veri seti üzerinde makine öğrenme metotlarıyla en iyi özelliklerin analiz edilmesi sağlanmıştır.

Daha önce farklı veri setleri kullanılarak yapılan çalışmalarda %100'e yakın bir başarı oranıyla elde edilen sonuçların Random Forest ve SVM algoritmaları olduğu Çizelge 6.1'de görülmüştür.

Çizelge 6.1 Veri setlerinde kullanılan algoritmalar ve başarı oranları

Veri Seti	Logistic Regresyon	Gaussian NaiveBayes	k-nearest neighbor	Bernoulli Naive Bayes	Decision Tree	Random Forest	SVM
1. Veri Seti	0.997	0.755	0.987	0.923	0.988	0.947	0.998
2. Veri Seti	0.791	0.992	0.994	0.992	0.977	0.997	0.981
3. Veri Seti	0.883	0.585	0.882	0.872	0.963	0.996	0.973
4. Veri Seti	0.914	0.786	0.964	0.723	0.979	0.993	0.992
5. Veri Seti	0.998	0.987	0.988	0.948	0.991	0.998	0.97

Çizelge 6.2 Dört özellik ile elde edilen recall, f1 ve precision değerleri

Birinci Veri Seti	0	0	0	1	1	1
Algoritma	**precision**	**recall**	**f1-score**	**precision**	**recall**	**f1-score**
Logistic Regresyon	1.00	0.99	0.99	0.99	1.00	0.99
Gaussian	1.00	0.99	0.99	0.99	1.00	0.99

NaiveBayes						
k-nearest neighbor	1.00	1.00	1.00	1.00	1.00	1.00
Bernoulli Naive Bayes	1.00	0.99	0.99	0.99	1.00	0.99
Decision Tree	1.00	1.00	1.00	1.00	1.00	1.00
RandomForest	1.00	1.00	1.00	1.00	1.00	1.00
SVM	1.00	0.99	0.99	0.99	1.00	0.99

Çizelge 6.3 Altı özellik ile elde edilen recall, f1 ve precision değerleri

İkinci Veri Seti	0	0	0	1	1	1
Algoritma	**precision**	**recall**	**f1-score**	**precision**	**recall**	**f1-score**
Logistic Regresyon	1.00	0.99	0.99	0.99	1.00	0.99
Gaussian NaiveBayes	0.99	0.99	0.99	0.99	0.99	0.99
k-nearest neighbor	1.00	1.00	1.00	1.00	1.00	1.00
Bernoulli Naive Bayes	1.00	0.99	0.99	0.99	1.00	0.99
Decision Tree	1.00	1.00	1.00	1.00	1.00	1.00
RandomForest	1.00	1.00	1.00	1.00	1.00	1.00
SVM	1.00	0.99	0.99	0.99	1.00	0.99

Çizelge 6.4 Sekiz özellik ile elde edilen recall, f1 ve precision değerleri

Üçüncü Veri Seti	0	0	0	1	1	1
Algoritma	**precision**	**recall**	**f1-score**	**precision**	**recall**	**f1-score**
Logistic Regresyon	0.94	0.82	0.88	0.84	0.95	0.89
Gaussian NaiveBayes	0.55	1.00	0.71	1.00	0.17	0.29
k-nearest neighbor	0.99	0.99	0.99	0.99	0.99	0.99
Bernoulli Naive Bayes	0.93	0.81	0.86	0.83	0.94	0.88
Decision Tree	0.99	0.99	0.99	0.99	0.99	0.99
RandomForest	0.99	0.99	0.99	0.99	0.99	0.99
SVM	0.94	0.83	0.88	0.85	0.95	0.89

Çizelge 6.5 On özellik ile elde edilen recall, f1 ve precision değerleri

Dördüncü Veri Seti	0	0	0	1	1	1
Algoritma	**precision**	**recall**	**f1-score**	**precision**	**recall**	**f1-score**
Logistic Regresyon	0.96	0.86	0.91	0.87	0.97	0.92
Gaussian NaiveBayes	0.95	0.61	0.74	0.71	0.96	0.82
k-nearest neighbor	1.00	0.99	0.99	0.99	1.00	0.99
Bernoulli Naive Bayes	0.74	0.68	0.71	0.71	0.76	0.73
Decision Tree	1.00	1.00	1.00	1.00	1.00	1.00
Random Forest	1.00	1.00	1.00	1.00	1.00	1.00
SVM	0.96	0.82	0.88	0.84	0.97	0.90

Çizelge 6.6 On iki özellik ile elde edilen recall, f1 ve precision değerleri

Beşinci Veri Seti	0	0	0	1	1	1
Algoritma	**precision**	**recall**	**f1-score**	**precision**	**recall**	**f1-score**
Logistic Regresyon	0.92	0.81	0.75	0.65	0.66	0.85
Gaussian NaiveBayes	0.98	1.00	0.99	1.00	0.98	0.99
k-nearest neighbor	1.00	1.00	1.00	1.00	1.00	1.00
Bernoulli Naive Bayes	1.00	1.00	1.00	1.00	1.00	1.00
Decision Tree	1.00	1.00	1.00	1.00	1.00	1.00
RandomForest	1.00	1.00	1.00	1.00	1.00	1.00
SVM	1.00	1.00	1.00	1.00	1.00	1.00

Çalışmada kullanılan veri setiyle ilk yapılan çalışmada Random Forest Algoritması ile 11 çeşit DDOS atağının tespit edilmesinde belirleyici olan özellikler ortaya çıkarılmıştır. Bu tez çalışmasında ise farklı algoritmalar ile güncel veri seti olan CICDDoS2019 veri setinde yer alan tehdit türlerinin tespitinde kullanılabilecek en iyi özellikleri bulabilmek için Brute Force yöntemi

kullanılarak farklı 4, 6, 8, 10 ve 12 özelliğe sahip toplamda her kategoriden 50'şer adet alınan veri setleri oluşturulmuştur. Herbir veri seti üzerinde YSA, Gaussian Naive Bayes, Multinomial Naive Bayes, Bernoulli Naive Bayes, Logistic Regresyon, K-nearest neighbour (KNN), Decision Tree (entropy-gini), Random Forest ve SVM algoritmaları kullanılarak eğitilmiştir.

Çalışmada elde edilen sonuçlarda;

- Eğitim ve test için kullanılan veri setleriyle en yüksek başarı oranı K-nearest neighbor, Logistic Regrasyon, Naive Bayes, (Multinomial - Bernoulli) algoritmaları kullanılarak gerçekleştirilen algoritmalarla sağlandığı,
- Eğitim ve test süreleri göz önüne alındığında ise SVM algoritması ile %99,7 gibi yüksek bir oranda saldırı tespiti gerçekleştirilmiş ve performansının en iyi olduğu,
- Farklı algoritmalar ile eğitimi gerçekleştirilen veri içerisinden en yüksek doğruluk oranı sonuçlarını veren 5 veri seti analiz edilerek Fwd Pkt Len Std, Fwd Seg Size Min, Bwd Pkt Len Std, Bwd Pkt Len Min, CWE Flag Count, Bwd Seg Size Avg, Bwd Seg Size Min özelliklerinin DDOS saldırılarının tespitinde en belirgin değerler olduğu,
- Eğitim ve test verisi olarak kullanılan veri setlerinde en yüksek başarı oranları 0,3 f değeri kısaca yüzde 30 test verisi kullanılarak elde edildiği

görülmüştür.

CICDDoS2019 veri seti kullanılarak farklı makine öğrenme metotlarıyla gerçekleştirilen eğitimlerden sonuç olarak veri setleri içerisinde bulunan özelliklerden en iyi sonuç alınan değerlerin Fwd Pkt Len Std, Fwd Seg Size Min, Bwd Pkt Len Std, Bwd Pkt Len Min, CWE Flag Count, Bwd Seg Size Avg, Bwd Seg Size Min değerleriyle yapılan eğitimler olduğu ve STS tasarımlarında söz konusu özelliklerin gözönünde bulundurulması gerektiği düşünülmektedir.

KAYNAKLAR

Akkaya, E., 2020. IPS/IDS Nedir?, Erişim Tarihi: 05.06.2020 https://www.prismacsi.com/ips-ids-nedir/

Anderson, C., J., 1980. Computer Security Threat Monitoring and Surveillance. Fort Washington, Pennsylvania.

Anderson, D., Lunt, T., Javitz, H., Tamaru, A., Valdes, A., 1995. Detecting Unusual Program Behavior Using The Statistical Component of The Next-Generation Intrusion Detection Expert System, NIDES. Computer Science Laboratory, SRI International. California: SRI-CSL-95-06.

Axelsson, S., 2000a. Intrusion Detection Systems: A Survey and Taxonomy. Technical Report 99-15, Dept. of Computer Eng., Chalmers University of Technology, 1-23. Göteborg, Sweden.

Axelsson, S., 2000b. Intrusion detection systems: A survey and taxonomy. Technical Report (s. 1-23). Göteborg, Sweden: https://neuro.bstu.by/ai/To-dom/My_research/Paper-0-again/For-research/D-mining/Anomaly-D/Intrusion-detection/taxonomy.pdf.

Axelsson, S. 2000c. Intrusion Detection Systems: A Survey and Taxonomy. Department of Computer Engineering , Chalmers University of Technology. Göteborg: https://neuro.bstu.by/ai/To-dom/My_research/Paper-0-again/For-research/D-mining/Anomaly-D/Intrusion-detection/taxonomy.pdf.

Aydın, M., A., 2005. Bilgisayar Ağlarında Saldırı Tespiti İçin İstatistiksel Yöntem Kullanılması. İstanbul Teknik Üniversitesi, 1-125.

Bace, R., 1999. An Introduction to Intrusion Detection & Assessment. Pennsylvania: ICSA Technical Report.

Bace, R., Mell, P., 2001. Intrusion Detection Systems. NIST Special Publication on Intrusion Detection Systems, 800-31.

Başaranoğlu, E., 2020 siberportal. siberportal, Erişim Tarihi: 07.09.2020 https://www.siberportal.org/green-team/constructing-network-environment/tcp-three-way-handshake/

Baykal, A., 2006. Veri Madenciliği Uygulama Alanları. D.Ü.Ziya Gökalp Eğitim Fakültesi Dergisi, 95-107.

Baykara, M., 2016a. Bilişim Sistemleri İçin Saldırı Tespit ve Engelleme Yaklaşımlarının Tasarımı ve Gerçekleştirilmesi. Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Elazığ. . https://acikerisim.firat.edu.tr/xmlui/bitstream/handle/11508/20773/424189.pdf?sequence=1&isAllowed=y.

Baykara, M., 2016b. Bilişim Sistemleri İçin Saldırı Tespit ve Engelleme Yaklaşımlarının Tasarımı ve Gerçekleştirilmesi. Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Elazığ. . https://acikerisim.firat.edu.tr/xmlui/bitstream/handle/11508/20773/424189.pdf?sequence=1&isAllowed=y.

Baykara, M., Daş, R., 2019. Saldırı tespit ve engelleme araçlarının incelenmesi. DÜMF Mühendislik Dergisi , 57-75.

Belgiu, M., Draguţ, L., 2016. Random forest in remote sensing: A review of applications and future direction. ISPRS Journal of Photogrammetry and Remote Sensing, s. 24-31.

Christoph, G., J., 1995. UNICORN: Misuse Detection for UNICOS. Proceedings of the 1995 ACM/IEEE conference on Supercomputing, (s. 56-80). San Diego, California, United States.

CyberSecurity, C., I., 2019. Erişim Tarihi: 01/01/2019 unb.ca/cic/datasets/ddos-2019. unb.ca: https://www.unb.ca/cic/datasets/ddos-2019.html

Çavuşoğlu, Ü., Kaçar, S., 2019. Anormal Trafik Tespiti için Veri Madenciliği Algoritmalarının Performans Analizi. Academic Platform Journal of Engineering and Science, 205-216.

Dayıoğlu, B., 2001. Use Of Passive Network Mapping To Enhance Network Intrusion Detection. Dept. of Computer Engineering, Middle east Technical University. Ankara: The Graduate School Of Natural And Applied Sciences of The Middle East Technical University.

Denning, E., D., 1986. An Intrusion Detection Model. Proceedings of the Seventh IEEE Symposium on Security and Privacy, 119-131.

Evans, D., 2016. The Internet of Things. CISCO.

Fırlar, T., 2003. Ağ Güvenliği. SAU Fen Bilinıleri Enstitüsü Dergisi, 12.

Gökırmak Y., B. O. 2011. Sanal IPv6 Balküpü Ağı Altyapısı: Kovan. Ulusal IPv6 Konferansı.

Güven, E., N., 2007a. Zeki Saldırı Tespit Sistemlerinin İncelenmesi, Tasarımı ve Gerçekleştirilmesi. Yüksek Lisans Tezi, Fen Bilimleri Enstitüsü, Gazi Üniversitesi.

Güven, E., N., 2007b. Zeki Saldırı Tespit Sistemlerinin İncelenmesi, Tasarımı ve Gerçekleştirilmesi. Yüksek Lisans Tezi, Fen Bilimleri Enstitüsü, Gazi Üniversitesi .

Güven, E., N., 2007c. Zeki Saldırı Tespit Sistemlerinin İncelenmesi, Tasarımı Ve Gerçekleştirilmesi . Fen Bilimleri Ensititüsü , Gazi Üniversitesi . Ulusal Tez Merkezi .

Hatipoğlu, E., 2018. Erişim Tarihi: 01.07.2018 medium.com: https://medium.com/@ekrem.hatipoglu/machine-learning-classification-naive-bayes-part-11-4a10cd3452b4

Hosting. 2020. SMTP Nedir? Hosting, Erişim Tarihi: 21.07.2020 https://www.hosting.com.tr/bilgi-bankasi/smtp-nedir/

Ilgun, K., 1993. Ustat: A real-time intrusion detection system for Unix. Proceedings of the 1993 IEEE Symposium on Research in Security and Privacy, (s. 16-28). Oakland, California.

Internet of Things. 2016, Erişim Tarihi: 15.09.2020 cisco.com: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

lnxmaster.com. 2020, lnxmaster.com, Erişim Tarihi: 25.05.2020 https://lnxmaster.com/Makaleler/IDS-IPS.aspx

Karimkhani, R., Erişim Tarihi: 20.07.2020. medium: https://medium.com/@ramin_karimhani/dns-domain-name-system-nedi%CC%87r-ve-nasil-%C3%A7ali%C5%9Fir-465513138670

Kaşıkçı, T., Gökçen, H., 2014. Metin Madenciliği ile E-Ticaret Sitelerinin Belirlenmesi. BİLİŞİM TEKNOLOJİLERİ DERGİSİ, 25-32.

Kaya, Ç., Yıldız, O., 2014. Makine Öğrenmesi Teknikleriyle Saldırı Tespiti: Karşılaştırmalı Analiz. Marmara Fen Bilimleri Dergisi, 89-104.

Lunt, F., T., 1990. IDES: An Intelligent System for Detecting Intruders. Proceedings of the Symposium on Computer Security; Threats, and Countermeasures, 110-121.

M., E., 2005. Saldırı Tespit Sistemlerinde İstatistiksel Anormallik Belirleme Kullanımı.

Millî Eğitim Bakanlığı. Meslekî ve Teknik Eğitim Programlar ve Öğretim Materyalleri. 2011.

Mrutyunjaya Panda, M., R., 2007. Network Insrusipn Detection Using Naive Bayes. IJCSNS International Journal of Computer Science and Network Security.

Özekes, S., Karakoç, E., N., 2019. Makine Öğrenmesi Yöntemleriyle Anormal Ağ Trafiğinin Tespit Edilmesi. Düzce Üniversitesi Bilim ve Teknoloji Dergisi, 566-576.

Öztemel, E., 2006. Yapay Sinir Ağları. İstanbul: Papatya Yayıncılık.

Peddabachigari, S., A., 2007. Modeling intrusion detection system using hybrid intelligent systems. Journal of Network and Computer Applications, 30-114.

Pehlivanoğlu, M., K., Atay, R., Odabaş, D. E. 2019. İki Seviyeli Hibrit Makine Öğrenmesi Yöntemi ile Saldırı Tespiti. Gazi Mühendislik Bilimleri Dergisi, 258-272.

Pesen, M., M., 2020. sibergah, Erişim Tarihi: 19.07.2020 http://www.sibergah.com/genel/internet-guvenligi/ipv4-ipv6-guvenlik-karsilastirmasi-ipv6daki-degisiklikler/

Ratinder, K., Maninder, S. 2014. Efficient hybrid technique for detecting zero-day polymorphic worms. IEEE International.

Sağıroğlu, Ş., Yolaçan, E., N., Yavanoğlu, U. 2011. Zeki Saldırı Tespit Sistemi Tasarımı Ve Gerçekleştirilmesi. Gazi Üniv. Müh. Mim. Fak. Der., 26(2), 325-340.

Sağıroğlu, Ş., Yolaçan, E., N., Yavanoğlu, U. 2011. Zeki Saldırı Tespit Sistemi Tasarımı ve Gerçekleştirilmesi. Gazi Üniv. Müh. Mim. Fak. Der., 325-340.

Sancak, S., 2008. Saldırı Tespit Sistemi Tekniklerinin Karşılaştırılması. Yüksek Lisans Tezi, Sosyal Bilimler Enstitüsü, Gebze Yüksek Teknoloji Enstitüsü.

Sharafaldin, I., Friends, H., 2019. Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy.

Shital K. Ajagekar, V., J., 2016. Study on Web DDOS Attacks Detection Using Multinomial Classifier. IEEE International Conference on Computational Intelligence and Computing Research (ICCIC).

Söğüt, E., Erdem, O., A., Çetin, A., 2017. Saldırı Tespit Sistemlerinde Ajan Sistemlerin Kullanımı. 10. Uluslararası Bilgi Güvenliği Ve Kriptoloji Konferansı (s. 52). Ankara: https://www.researchgate.net/publication/333561955_Saldiri_Tespit_Sistemlerinde_Ajan_Sistemlerin_Kullanimi__Using_Agent_System_in_Intrusion_Detection_System.

Şen, ismailsen. ismailsen: Erişim Tarihi: 26.07.2020 http://ismailsen.com.tr/ag-tarama-analiz-saldirilari/

Tanrıkulu, H., Sazlı, M., H., 2007. Saldırı Tespit Sistemlerinde Yapay Sinir Ağlarının Kullanılması.

Turner, C., Jeremiah, R., Richards, D., Joseph, A., 2016. A Rule Status Monitoring Algorithm for Rule-Based Intrusion Detection and Prevention Systems . Procedia Computer Science, 361-368.

Tutar, M., M., kod5. Erişim Tairihi: 20.07.2020 kod5: https://kod5.org/basit-ag-yonetim-protokolu-snmp-nedir/

UNB, 2019. DDoS Evaluation Dataset (CICDDoS2019). Canadian Institute for Cybersecurity: Erişim Tarihi: 05.06.2020, https://www.unb.ca/cic/datasets/ddos-2019.html

Vaccarro, H., S., (1989). Detection of Anomalous Computer Session Activity. EEE Symposium on Research in Security and Privacy, 280-289.

Vikipedi, Erişim Tarihi: 05.07.2020, https://tr.wikipedia.org/wiki/Sald%C4%B1r%C4%B1_tespit_sistemleri#cite_note-1

Wani, A., R., Rana, Q. P., Saxena, U., N. Pandey. 2019. Analysis and Detection of DDoS Attacks on Cloud Computing Environment using Machine Learning Techniques. 2019 Amity International Conference on Artificial Intelligence (AICAI), (s. 870-875). Dubai, United Arab Emirates.

WikiPedia, Erişim Tarihi: 19.05.2020 https://tr.wikipedia.org/. https://tr.wikipedia.org/wiki/Metin_madencili%C4%9Fi:

WikiPedia, Erişim Tarihi:19.05.2020, https://tr.wikipedia.org/wiki/Uzman_sistemler

Yang, H., Li, T., Hu, X., Wang, F., Zou, Y. (1-11). A Survey of Artificial Immune System Based Intrusion Detection. The Scientific World Journal, 2014.

Zainal, A., Maarof, M. A., Shamsuddin, S., M., 2009. Ensemble Classifiers for Network Intrusion Detection System. Journal of Information Assurance and Security, 217-225.

ÖZGEÇMİŞ

Adı Soyadı : Tuğba AYTAÇ

Doğum Yeri ve Yılı : Berlin, 07/04/1993

Medeni Hali : (Bekar)

Yabancı Dili : İngilizce

E-posta : tugba.aytac@istanbulticaret.edu.tr

Eğitim Durumu

Lise : Bigadiç Anadolu Lisesi, 2011

Lisans : Süleyman Demirel Üniversitesi, Mühendislik Fakültesi, Elektronik ve Haberleşme Mühendisliği

Yüksek Lisans : İstanbul Ticaret Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği, 2020.

Mesleki Deneyim

Turkcell,
Ağ ve Güvenlik Mühendisi 2017-2018

Anadolubank,
Bilgi Teknolojileri Müfettişi 2018-…(devam ediyor)

Yayınları

Aytaç, T., Aydın, M.A., Zaim, A.H.,2020. Detection DDOS Attacks Using Machine Learning Methods. Electrica, 20(2), 159-167.