



T.C.
KONYA TEKNİK ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ



DAĞITIK HİZMET AKSATMA (DDoS)
SALDIRILARININ YAPAY ZEKA
YÖNTEMLERİ KULLANILARAK TESPİTİ

İlknur KAYACAN

YÜKSEK LİSANS TEZİ

Bilgisayar Mühendisliği Anabilim Dalı

MAYIS-2024
KONYA

TEZ KABUL VE ONAYI

İlknur KAYACAN tarafından hazırlanan “DAĞITIK HİZMET AKSATMA (DDOS) SALDIRILARININ YAPAY ZEKA YÖNTEMLERİ KULLANILARAK TESPİTİ” adlı tez çalışması 02/05/2024 tarihinde aşağıdaki jüri tarafından oy birliği / ~~oy çokluğu~~ ile Konya Teknik Üniversitesi Lisansüstü Eğitim Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı’nda YÜKSEK LİSANS/~~DOKTORA-TEZİ~~ olarak kabul edilmiştir.

Jüri Üyeleri

İmza

Başkan
Prof. Dr. Mesut GÜNDÜZ

.....

Danışman
Doç. Dr. Ahmet BABALIK

.....

Üye
Dr. Öğr. Üyesi Onur İNAN

.....

Yukarıdaki sonucu onaylarım.

Prof. Dr. Mevlüt UYAN
Enstitü Müdürü

TEZ BİLDİRİMİ

Bu tezdeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edildiğini ve tez yazım kurallarına uygun olarak hazırlanan bu çalışmada bana ait olmayan her türlü ifade ve bilginin kaynağına eksiksiz atıf yapıldığını bildiririm.

DECLARATION PAGE

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

İlknur KAYACAN

Tarih: 02.05.2024

ÖZET

YÜKSEK LİSANS TEZİ

DAĞITIK HİZMET AKSATMA (DDOS) SALDIRILARININ YAPAY ZEKA YÖNTEMLERİ KULLANILARAK TESPİTİ

İlknur KAYACAN

Konya Teknik Üniversitesi
Lisansüstü Eğitim Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı

Danışman: Doç. Dr. Ahmet BABALIK

2024, 75 Sayfa

Jüri

Prof. Dr. Mesut GÜNDÜZ
Doç. Dr. Ahmet BABALIK
Dr. Öğr. Üyesi Onur İNAN

İnternet her geçen gün hayatımızda daha çok alana nüfuz etmektedir. Ancak beraberinde güvenlik problemleriyle daha çok karşılaşmaya başlanmıştır. Nexuesquard'ın 2023 yılının ilk çeyreği için yayınladığı rapora göre Dağıtık Hizmet Aksatma (DDoS) saldırılarının %183 oranında arttığı raporlanmıştır (Anonim, 2023a). Aynı zamanda Nesnelerin İnternet'i uygulamalarıyla internete katılan cihaz sayısı arttıkça saldırganların saldırı ağlarının kapasitesi genişlemektedir. İnternet ortamında güvenliği sağlamak için dönemin tekniklerine uygun olarak yapay zekâ temelli saldırı tespit sistemleri inşa edilmektedir.

Bu çalışmanın amacı saldırı tespit sistemlerinde kullanılan öznelilikleri karşılıklı bilgi metodu ile seçip yapay zekâ temelli algoritmalarının DDoS ataklarını tespit etme başarı oranlarını analiz ederek gelişmiş saldırı tespit sistemleri oluşmasına katkı sağlamaktır. Çalışmada CICDDoS2019 veri seti kullanılmıştır. Veri setinde yer alan DDoS atakları makine öğrenmesi algoritmaları olan K-En Yakın Komşu, Karar Ağacı, Naive Bayes ve Rasgele Orman algoritmaları kullanılarak tespit edilmiştir. Çalışma kapsamında yapılan tüm deneylerde öznelilik seçiminden sonra yapılan sınıflandırma başarısında kabul edilebilir seyide düşüş gözlenmiştir, tespit sürelerinde ise belirgin bir azalma gözlenmiştir. Gerçek hayat uygulamalarında ağ trafiğinin yönetiminde atakların türüne bakılmaksızın engellenmesi, atak olmayan paketlerin ise ağ trafiğine dahil edilmesi beklenir. Tüm öznelilikler kullanılarak gerçekleştirilen ikili sınıflandırma işleminde test setinde atak olmayan paketlerin tespitinde doğruluk oranı %99,34 ile K-En Yakın Komşu algoritmasında elde edilmiştir, öznelilik seçimi yapıldıktan sonra ise en yüksek doğruluk oranı %96,29 ile Naive Bayes algoritmasında elde edilmiştir. Sınıflandırmada kullanılan öznelilik sayısının azaltılması hafıza kullanımı ve CPU işlem zamanında azalma sağlaması beklenir. Yapılan deneysel çalışmada buna paralel olarak öznelilik seçimi yapıldıktan sonra yapılan sınıflandırma işlem sürelerinde belirgin bir azalma olduğu gözlenmiştir.

Anahtar Kelimeler: Bilgi Güvenliği, DoS-DDoS tespit sistemleri, Karşılıklı bilgi metodu, İnternet güvenliği, Saldırı tespit sistemleri.

ABSTRACT

MS THESIS

DETECTION OF DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS USING ARTIFICIAL INTELLIGENCE METHODS

İlknur KAYACAN

**Konya Technical University
Institute of Graduate Studies
Department Of Computer Engineering**

Advisor: Assoc. Prof. Dr. Ahmet BABALIK

2024, 75 Pages

Jury

**Prof. Dr. Mesut GÜNDÜZ
Assoc. Prof. Dr. Ahmet BABALIK
Assist. Prof. Dr. Onur İNAN**

The Internet penetrates more and more areas of our lives every day. However, security problems have started to be encountered more and more. According to the report published by Nexuesquard for the first quarter of 2023, Distributed Denial of Service (DDoS) attacks increased by 183% (Anonymous, 2023a). At the same time, as the number of devices joining the Internet increases with Internet of Things applications, the capacity of attackers' attack networks is expanding. In order to ensure security in the Internet environment, artificial intelligence-based intrusion detection systems are being built in accordance with the techniques of the period.

The aim of this study is to contribute to the development of advanced intrusion detection systems by selecting the features used in intrusion detection systems with the mutual information method and analyzing the success rates of artificial intelligence-based algorithms in detecting DDoS attacks. CICDDOS2019 dataset was used in the study. DDoS attacks in the dataset were detected using machine learning algorithms such as K-Nearest Neighbor, Decision Tree, Naive Bayes and Random Forest algorithms. In all experiments conducted within the scope of the study, an acceptable decrease was observed in the classification success after feature selection, and a significant decrease was observed in detection times. In real-life network traffic management, it is expected that attacks are blocked regardless of their type and non-attack packets are included in the network traffic. In the binary classification process performed using all features, the accuracy rate in detecting non-attack packets in the test set was obtained in the K-Nearest Neighbor algorithm with 99.34%, and after the feature selection was made, the highest accuracy rate was obtained in the Naive Bayes algorithm with 96.29%. Reducing the number of features used in classification is expected to reduce memory usage and CPU processing time. In the experimental study, in parallel with this, a significant reduction in the classification processing time after feature selection was observed.

Keywords: Information Security, DoS - DDoS detection systems, Mutual information method, Internet security, Intrusion detection system

ÖNSÖZ

Bu tez çalışmasının araştırılmasında ve yürütülmesinde her daim destek olan ve her durumda yardımını esirgemeyen değerli danışman hocam Sayın Doç. Dr. Ahmet BABALIK’a, tez çalışması süresince beni destekleyen aileme teşekkürlerimi sunuyorum.

İlknur KAYACAN

KONYA-2024



İÇİNDEKİLER

TEZ BİLDİRİMİ.....	ii
ÖZET	iii
ABSTRACT	iv
ÖNSÖZ	v
İÇİNDEKİLER	vi
KISALTMALAR.....	viii
1. GİRİŞ	1
2. KAYNAK ARAŞTIRMASI.....	5
3 MATERYAL VE YÖNTEM	5
3.1. Bilgisayar Ağı Nedir?.....	8
3.2. TCP/IP Protokol Kümesi.....	8
3.2.1. Ağ erişim katmanı	9
3.2.2. İnternet katmanı.....	9
3.2.3. Taşıma katmanı	9
3.2.4. Uygulama Katmanı.....	9
3.3. Ağ Sisteminde Güvenlik Kavramı	10
3.4. Saldırı Yöntemleri	11
3.5. Saldırı Tespit Sistemleri (STS).....	15
3.5.1. İmza tabanlı saldırı tespit yöntemi (Signature detection).....	16
3.5.2. Anomali tabanlı saldırı tespit yöntemi (Anomaly detection)	17
3.5.3. Durumsal protokol analizi saldırı tespit yöntemi (Protocol analysis).....	18
3.6. Saldırı Tespit Sistem Mimarileri	19
3.6.1. Ana bilgisayar tabanlı STS mimarisi (Host Based Intrusion Detection System-HIDS)	19
3.6.2. Ağ tabanlı STS mimarisi (Network Intrusion Detection System-NIDS).....	19
3.6.3. Kablosuz ağ tabanlı STS mimarisi (Wireless Intrusion Detection System-WIDS)	20
3.6.4. Ağ davranışı temelli analiz mimarisi (Network Behavior Analise)	20
3.6.5. Derin öğrenme tabanlı mimari (Deep Learning Detection).....	20
3.7. Dağıtık Hizmet Aksatma (DDoS) Atağı Nedir?	21
3.8. DDoS Atağı Örnekleri.....	23
3.9. DDoS Atak Yöntemleri	26
3.9.1. Volümetrik (Amplification) atakları	26
3.9.2. Protokol atakları	27

3.9.3. Uygulama katmanı atakları.....	28
3.10. DDoS Atak Çeşitleri.....	28
3.10.1. UDP seli atağı.....	29
3.10.2. SYN (Neptun) seli atağı	30
3.10.3. ICMP seli atağı.....	31
3.10.4. DNS kuvvetlendirmeli DDoS atağı	31
3.10.5. NTP kuvvetlendirmeli DDoS atağı.....	32
3.10.6. SNMP kuvvetlendirmeli DDoS atağı.....	32
3.10.7. Character Generator Protocol (CharGEN) atağı	33
3.11. CICDDOS2019 Veri Seti	33
3.12. Veri Önileme	36
3.12.1. Öznitelik seçimi.....	36
3.13. K En Yakın Komşu (KNN) Algoritması	40
3.14. Naive Bayes (NB) Algoritması.....	42
3.15. Rasgele Orman (RF) Algoritması.....	43
3.16. Karar Ağacı Algoritması (DT).....	45
4. ARAŞTIRMA BULGULARI VE TARTIŞMA.....	47
4.1. Performans Metrikleri	47
4.2. Deneysel Sonuçlar	48
4.2.1. K en yakın komşu algoritması kullanılarak elde edilen sonuçlar	49
4.2.2. Naive Bayes (NB) algoritması kullanılarak elde edilen sonuçlar.....	53
4.2.3. Rasgele Orman (RF) algoritması kullanılarak elde edilen sonuçlar	56
4.2.4. Karar ağacı (DT) algoritması kullanılarak elde edilen sonuçlar.....	60
4.2.5. Algoritmaların performanslarının karşılaştırılması	64
5. SONUÇLAR VE ÖNERİLER.....	67
KAYNAKLAR	69

KISALTMALAR

ARPANET	: The Advanced Research Projects Agency Network
IoT	: Nesnelerin İnterneti
DDoS	: Distributed Denial of Services
DoS	: Denial of Services
KNN	: k-Nearest Neighbor
ML	: Machine Learning
RF	: Random Forest
SaE-ELM	: Self-Adaptive Evolutionary Extreme Learning Machine
IDS	: Intrusion Detection System
STS	: Saldırı Tespit Sistemi
DT	: Decision Tree
YSA	: Yapay Sinir Ağları
MV	: Majority Voting
IP	: Internet Protocol
TCP	: Transmission Control Protocol
HIDS	: Host-Based Intrusion Detection System
NIDS	: Network Intrusion Detection System
WIDS	: Wireless Intrusion Detection System
BT	: Bilgi Teknolojileri
HTTP	: Hyper Text Transfer Protocol
RPS	: Request per second
SOC	: Security Operations Center
GBPS	: Gigabit per second
TBPS	: Terabit per second
ISP	: Internet Service Provider
LDAP	: Connection-less Lightweight Directory Access Protocol
DNS	: Domain Name Server
SMTP	: Simple Mail Transfer Protocol
AWS	: Amazon Web Service

OVH	: Online Virtual Hosting
UDP	: User Datagram Protocol
NTP	: Network Time Protocol
OSI	: Open System Interconnection
ISO	: International Organization for Standardization
SYN	: Synchronize
ACK	: Acknowledge
URL	: Uniform Resource Locator
SNMP	: Simple Network Management Protocol
SSDP	: Simple Services Discovery Protocol
LDAP	: Lightweight Directory Access Protocol
TFTP	: Trivial File Transfer Protocol
ROC	: Receiver Operator Characteristic Curve

1. GİRİŞ

Bilgisayar ağı kavramı 1960'lı yılların başında ABD askeri teşkilatının iletişim sorununa çözüm olarak ortaya çıkmıştır. Dünyaya yayılarak tekli yapıdan çoklu yapıya geçmesiyle internet yapısı meydana gelmiştir. İnternet kavramı “Ağların Ağı” olarak bilişim sektöründe yerini almıştır. Bilgisayar ağı mimarisinin ilk dizaynları ABD, Fransa ve İngiltere'deki laboratuvarlarda üretilmiştir. Literatürde ise birden fazla cihazın anladıkları, üzerinde anlaştıkları bir dil ile (protokol) karşılıklı olarak veri alış-verişinde bulundukları ve veri akışının olduğu ortam olarak tanımlanır (Aktaş, 2018). Diğer bir kaynakta ise makine sistemlerini birbirine bağlayan elektronik iletişim ağı olarak tanımlanmıştır (Toprak ve ark., 2009).

1969'dan sonra ABD savunma sistemi için geliştirilen The Advanced Research Projects Agency Network kısa adıyla ARPANET dünyanın çeşitli üniversiteleriyle paylaşılmıştır. Bu gelişmenin ardından bilgisayar ağına dahil olacak cihazlar için çeşitli protokoller geliştirilmiş ve birden çok bilgisayar ağının birleşmesiyle şu an ki internet halini almıştır.

ARPANET'in oluşturulmasındaki amaç iletişimi kolaylaştırmak ve güvenli bir şekilde bilgi aktarımı gerçekleştirmektir. Bu ağ üzerinde akan bilgiler, ABD savunma sistemine ait bilgiler olduğundan dolayı; diğer ülkelerin bu bilgilere ulaşmak istemeleri hatta ABD savunma teşkilatının içinde bulunan üyelerinin de casusluk girişimlerinde bulunma ihtimallerine karşı sistem güvenlik tehlikesiyle karşı karşıya kalmıştır. Bunu ilk fark eden ve bu konu hakkında makale yayınlamaya meseleyi bilimsel bir şekilde ele alan kişi John von Neumann'ın asistanı Willis Ware'dır. Yayınladığı “Security and Privacy in Computer Systems” başlıklı çalışmasında bilgisayar ağı sistemleri için oluşabilecek tehlikeleri ele almıştır (Ware, 1967).

ARPANET'in geliştirildiği dönemde tek bir ağ olması ve dünya çapında yayılmaması nedeniyle güvenlik problemleriyle karşılaşılmamıştır. Ancak teknolojinin paylaşılması, bilgisayar ağlarının birbirleriyle birleşmeye başlaması ve beklenenden daha hızlı bir şekilde yayılması sonucu çeşitli güvenlik sorunları baş göstermiştir. Aynı zamanda teknolojinin hızla gelişmesi, geliştirilen her protokolün kendi içinde zafiyetlere sahip olması, internet dünyasına katılan cihazların sayısının her geçen gün artması ve Nesnelerin İnterneti'nin (IoT) hızla yaygınlaşması internet dünyasında güvenlik problemlerini daha da arttırmıştır.

İnternetin insanlar ve cihazlar tarafından yaygın bir şekilde kullanılması, saldırganlar için büyük bir fırsattır. İnternetin ve internete bağlı cihazların hedef olarak gerçekleştirildiği bu tür saldırılar, siber saldırı olarak nitelendirilir. Microsoft tarafından yayınlanan rapora göre Dağıtık Hizmet Aksatma (DDoS) atakları son yıllarda sıklıkla tercih edilen siber saldırı çeşitleri

arasında yer almaktadır (Anonim, 2022b). DDoS atağının temel amacı hedef sistemi kullanılamaz ya da erişilemez hale getirmektir.

DDoS ataklarını diğer siber ataklardan ayıran en önemli nitelikleri maliyetinin düşük olması ve güvenlik ürünleri tarafından da engellenmesinin oldukça güç olmasıdır. DDoS atakları sırasında en önemli bileşenler; Robot Network (BotNet) olarak bilinen saldırganın zararlı yazılımlar aracılığıyla kurmuş olduğu ağ, zombi cihaz konumuna getirilmiş olan cihazlar ve zafiyete açık legal sunuculardır. Günümüzde gelişen teknolojiye rağmen internetin girdiği her ortamda zafiyetinde yer almasından dolayı DDoS saldırılarının her zamankinden daha çok gündemde olması beklenmektedir. Siber tehditleri izlemek ve analiz etmek amaçlı kurulan uluslararası bir kuruluş olan Spamhaus'un 2023 yılının 1. çeyreğinde yayınlamış olduğu BotNet Tehdit Güncellemesi raporuna göre BotNet komuta ve kontrol (C&C) sunucularının sayısı %23 oranında artmıştır. Çizelge 1.1'de gözlemlenebilen BotNet C&C sunucularının 2022 yılının son çeyreğinden 2023 yılının ilk çeyreğine en çok artış yaşadığı ülkeler ve artış miktarları verilmektedir (Anonim, 2022b).

Çizelge: 1.1 BotNet C&C sunucularının ülkelere göre sayısı

Çeyrek	Q4 2022	Q1 2023	2022 Q4 ile 2023 Q1 Arası %'lik Değişim
ABD	1713	1857	%+8
Çin	1033	993	%-4
Rusya	500	811	%+62
Hollanda	467	683	%+46
Almanya	391	609	%+56
Fransa	227	319	%+41
Birleşik Krallık	165	249	%+51
İsviçre	61	164	%+169
Kanada	148	154	%+4
Singapur	125	152	%+22

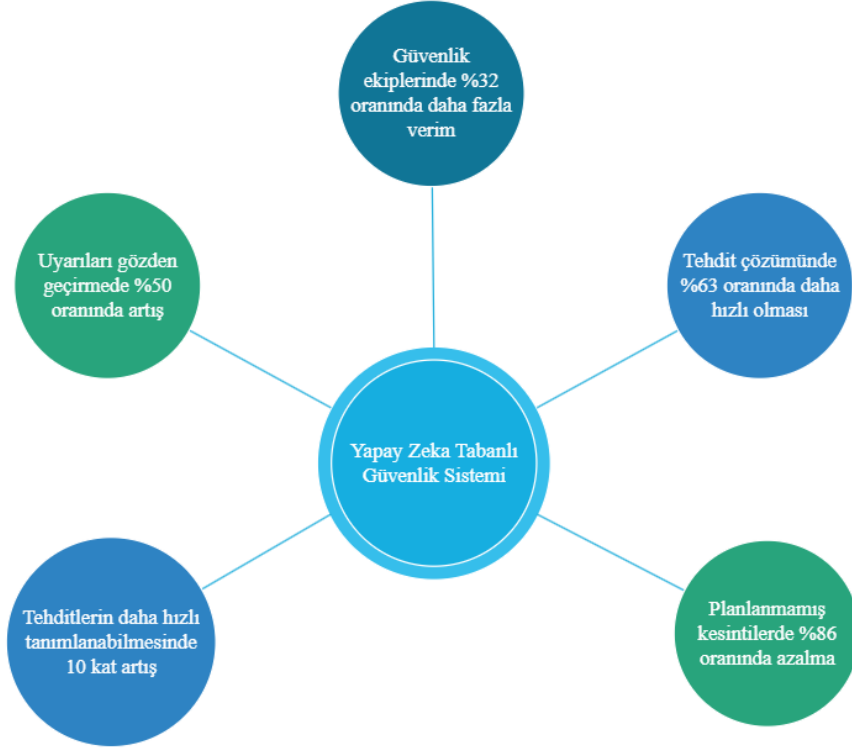
Rapora göre C&C sunucularının sayısındaki en yüksek artış %169 ile İsviçre'de görülmektedir. Bu artışı %62 ile Rusya takip etmektedir. Çin' de C&C sunucularının sayısında %4 oranında azalma meydana gelmiştir. BotNet'ler DDoS ataklarının en önemli parçası olduğundan dolayı BotNet C&C sunucularındaki artış DDoS ataklarının sayısında artışa sebep olabilir.

DDoS ataklarının son derece hızlı gerçekleşmesi ve oldukça büyük paket kapasitesine erişebilmesi, internet üzerinden servis sağlayan sistemlerin servis dışı kalmasına neden olmaktadır. Bununla birlikte saldırganlar normal kullanıcıların internet servislerine yoğun istek yaptığı zaman dilimlerini de kullanarak sunuculara DDoS atakları yapabilmektedirler. Nexusguard'ın 2023 yılının 1. çeyreğinde yayınladığı 2023 1. Çeyrek DDoS İstatistik Raporuna göre 2023 1. çeyrekte DDoS atakları %183,33 oranında büyümüştür (Anonim, 2023c).

Dolayısıyla internet üzerinden servis sağlayan bu sistemlerin güvenliği için kullandıkları ağı hızlı analiz edip, gerçek zamanlı tespitler yapıp atakları engelleyebilen sistemler tasarlanmalıdır.

Sürekli dikkat halinde kalamayan, değerlendirmesi gereken tüm parametreleri hesaba katmayı unutabilen, buna ek olarak da duygusal iniş ve çıkışları olan insan yapısını göz önüne aldığımızda dijital sistemlerin güvenlikleri, yapay zekâ temelli sistemler ile profesyonel bir şekilde sağlanabilir. Güvenlik duvarlarının, anti virüs programlarının standart yapıları göz önüne alındığında sistem ya manuel olarak ya belirli zamanlarda ya da yeni nesil virüs programları tarafından saldırıya uğradığında güncelleme işlemleri yapılmaktadır. Tüm bunlar dikkate alındığında sistemi sürekli inceleyen ve gerektiğinde aktif pozisyon alabilecek yapay zekâ temelli sistemleri sistem güvenliğinde etkin olabilirler. Güvenlik kriterlerinden olan hızlı tespit etmek, cihazların donanımsal ve yazılımsal olarak kapasitelerini aşacak her türlü eylemden kaçınmak ve olası sorunlara hızlı çözüm üretmek yapay zeka temelli güvenlik sistemleriyle verimli olarak yönetilebilir. Bir diğer önemli kriter ise tehditlerin hızlı algılanmasıdır. Geleneksel güvenlik sistemlerinde bir tehdidi algılamak için sistemin o tehdidi önceden tanıyor olması gerekir. Bu durum sistemleri yeni nesil zararlı yazılımlara karşı savunmasız hale getirir. Yapay zeka temelli güvenlik sistemleri ile yeni nesil tehditler algılanarak engellenebilir.

Winder (2019), yapay zekâ temelli bir güvenlik sisteminin %32 oranında kullanılan güvenlik ekipmanlarından verim sağladığı ve bu verim ile cihaz performansındaki düşüşün azaldığı, %63 oranında tehditlerin çözümünde daha hızlı olması ile sistemin tehditlere karşı oldukça aktif korunduğu, %50 oranında uyarıları dikkate alıp değerlendirmede artış sağlayarak sistemlerin olası problemlere erken müdahalede bulunarak devamlılığını sağladığı, %86 oranında rasgele gerçekleşen sistem kesintilerinde azalma olduğu ve tehditlerin tanımlanmasında 10 katlık bir artış olduğunu belirtmiştir. Şekil 1.1’de yapay zekâ temelli güvenlik sistemlerinin avantajları gösterilmektedir.



Şekil: 1.1 Siber güvenlikte yapay zekâ kullanımının avantajları

Bu çalışma kapsamında yapay zekâ temelli modeller olan K-En Yakın Komşu (KNN), Rasgele Orman (RF), Karar Ağaçları (DT) ve Naive Bayes (NB) algoritmalarının DDoS ataklarını tespit etme başarıları değerlendirilmiştir. Bu modellerin her birinin performans ve doğruluk değerleri karşılaştırılmış bunların neticesinde DDoS ataklarının tespitinin hızlanması ve sisteme büyük çaplı zararlar verilmeden atakların önlenmesine katkı sağlamak amaçlanmıştır.

Çalışma beş bölümden oluşmaktadır. “Giriş” bölümünde tezin kapsamı hakkında genel bilgilere yer verilmiştir. İkinci bölüm olan “Kaynak Araştırması” bölümünde DDoS saldırıları ile ilgili literatür çalışmalarına yer verilmiştir. Üçüncü bölüm olan “Materyal ve Yöntem” bölümünde bilgisayar ağ yapısından, TCP/IP protokol kümesinden, saldırı tespit sistemlerinden (STS), DDoS ataklarıyla ilgili genel bilgilerden ve istatistiklerden, kullanılan veri setinden, yapay zekâ modelleri anlatılmıştır. Dördüncü bölüm olan “Araştırma Sonuçları ve Tartışma” bölümünde deney ortamı, yapay zekâ modellerinin performansı ve sonuçları açıklanmıştır. Son bölüm olan “Sonuçlar ve Öneriler” kısmında ise çalışma özetlenerek sonuçlar değerlendirilmiş ve gelecekte nasıl çalışmalar yapılabilceğine değinilmiştir.

2. KAYNAK ARAŞTIRMASI

DDoS ataklarını tespit etmek amacıyla Makine Öğrenmesi (Machine Learning-ML) modellerinin kullanıldığı birçok çalışma yapılmıştır. Bu kısımda DDoS ataklarını tespit etmek amacıyla hazırlanmış veri setleri ile yapılan çalışmalar özetlenmektedir.

Alzahrani ve Hong (2018), DDoS ataklarını tespit etmek için imza tabanlı yaklaşımla birlikte yapay sinir ağları (YSA) modelini birleştirerek bir çalışma yapmışlardır. Deney sonucunda %99,98 oranında bir doğruluk oranına ulaşılmıştır.

Çebi ve arkadaşları (2019), makine öğrenmesi modelleri olan Karar Ağacı, Rastgele Orman, K-En Yakın Komşu, Adaboost, Gradyan Artırma, Doğrusal Ayrımcılık Analizi, Yapay Sinir Ağları algoritmaları kullanılarak geliştirilen Saldırı Tespit Sistem'lerinin (STS) doğruluk oranları NSL-KDD veri seti üzerinde eğitim süreleri ve çalışma performansları açısından birbirleriyle mukayese etmiştir. Bu çalışmaya göre KNN algoritmasının doğruluk oranı %95,18 olarak hesaplanmış ve diğer modellerden daha yüksek bir doğruluğa sahip olduğu görülmüştür.

Sambangi ve Gondi (2020), CICIDDoS2017 veri setini kullanarak bulut ortamında DDoS ataklarını tahmin etmek için bir makine öğrenmesi modeli oluşturmuşlardır. Bu çalışmada makine öğrenmesi modeli olarak çoklu regresyon analizi kullanılmıştır. Çalışmada çoklu regresyon modelinin doğruluk oranı %73,79 olarak belirlenmiştir.

Das ve arkadaşları (2020), ML tabanlı STS'ler ile DDoS ataklarının daha iyi tespit edildiğini ifade etmektedir. Özellik seçimini kullanarak DDoS atak tespiti yapılırken kullanılan öznitelikleri optimize ederek daha kısa sürede daha doğru sonuçlar almayı hedeflemişlerdir. Çalışmada çoğunluk oylama (Majority Voting- MV) tekniği kullanılarak öznitelik seçim yöntemleri için bir topluluk çerçevesi önerilmiştir. NSL-KDD veri seti kullanılarak deneyler gerçekleştirilmiştir. Destek Vektör Makinası algoritmasında %89, DT algoritmasında %97 ve NB algoritmasında %88 doğruluk değerleri tespit edilmiştir.

Saini ve arkadaşları (2020), DDoS ataklarının tespitinde, Mouhammd Alkasassbeh ve arkadaşları tarafından toplanan ve UDP seli, Http seli, Smurf ve SIDDoS ataklarını içeren veri seti üzerinde C4.5, YSA, RF ve NB algoritmaları kullanılmıştır. %98,64 oranıyla en yüksek doğruluk oranı C4.5 algoritmasında elde edilmiştir.

Thorat ve arkadaşları (2021), transport katmanı üzerinden gerçekleştirilen DDoS saldırılarını tespit etmek için yeni bir yaklaşım sunmuşlardır. Bu çalışmada ML kullanılarak CICIDDoS2019 veri seti üzerinde Taksonomi Tabanlı Böl ve Yönet (TaxoDaCML) yaklaşımıyla DDoS ataklarını %99,9 oranında tespit etmiş ve %85'ten fazla doğruluk

sağlamıştır. Buna göre de TaxoDaCML yaklaşımının önceki çalışmalarla karşılaştırılmasıyla DDoS atak sınıflandırması için daha iyi bir performans ortaya koymuştur.

Batchu ve Seetha (2021), DDoS saldırılarını tespit etmek amacıyla önceki yaklaşımlardan farklı olarak özneliliklerin sayısını azaltarak yeni bir otomatik algılama metodolojisi geliştirmişlerdir. Sınıflandırma doğruluğunu arttırıcı öznelilikler seçilerek Lojistik Regresyon, Gradyan Artırma, DT, KNN ve SVM algoritmaları ile seçilen parametreler test edilmiştir. Deneylerde CICDDoS2019 veri seti kullanılmıştır. Sonuçlarında ise Gradyan Artırma modelinin %99,97 oranıyla diğer yöntemlere kıyasla daha iyi bir performans gösterdiğini belirtmişlerdir.

Manjula ve Mangla (2021), sınıflandırma algoritmalarını kullanarak DDoS ataklarını tespit etmeyi amaçlamışlardır. Çalışmada Wireshark aracılığıyla elde edilen veri seti kullanılmıştır. Loic saldırı aracıyla saldırı başlatılmış ve tespit analizi için Apache Spark'a aktarılmıştır. Sistem veri kümesini sınıflandırmak için Apache Spark ML sınıflandırma algoritmalarını kullanmıştır. Normal trafiği ve saldırıya uğramış trafiği sınıflandırmak için NB, KNN ve RF sınıflandırma algoritmaları kullanılmıştır. Çalışmada DDoS saldırı tespitinin doğruluğu, üç sınıflandırma algoritması üzerinde karşılaştırılmış ve RF modelinin %96,75 doğruluğa sahip olduğu kaydedilmiştir.

Kushwah ve Ranga (2021), bulut bilişim üzerinden gerçekleşen DDoS ataklarına karşı savunma oluşturabilmek için geliştirilmiş kendinden uyarlamalı evrimsel aşırı öğrenme makinesine (SaE-ELM) dayalı bir DDoS saldırı tespit sistemi önermişlerdir. SaE-ELM modeli, iki özellik daha dahil edilerek geliştirilmiştir. İlk olarak, en uygun çaprazlama operatörü uyarlanır. İkinci olarak, uygun sayıda gizli katman nöronunu otomatik olarak belirlenir. Bu özelliklerin modelin öğrenme ve sınıflandırma yeteneklerini geliştirdiği bildirilmiştir. Önerilen sistem NSL-KDD, ISCX IDS 2012, UNSW-NB15 ve CICIDS2017 olmak üzere dört veri seti kullanılarak değerlendirilmiştir. NSL-KDD, ISCX IDS 2012, UNSW-NB15 ve CICIDS2017 veri setlerinde sırasıyla %86,80, %98,90, %89,17 ve %99,99 tespit doğruluğuna ulaşmışlardır.

Asarkaya ve arkadaşları (2021), DDoS ataklarını erken tespit etmeyi amaçlayan bir çalışma yapmışlardır. Bu çalışmada DDoS ataklarını tespit etmek için saldırılar makine öğrenmesi yöntemleriyle sınıflandırılmışlardır. Çalışmada Kaggle DDoS Attack Network Logs veri seti kullanılmıştır ve KNN, YSA, SVM ile RF sınıflayıcı modelleri kullanılarak deney yapılmıştır. En yüksek doğruluk oranına %99 başarı tespiti ile YSA modelinde ulaşılmıştır.

Alzahrani ve arkadaşları (2021), IoT ile birlikte saldırganların birçok yönden güçlendiğini düşünmektedirler. Bundan dolayı DDoS atakları tespitinde farklı ML algoritmalarını kullanmışlardır. CICDDoS2019 veri setini kullanarak KNN, Süper Vektör, NB,

DT, RF ve Lojistik Regresyon algoritmaları değerlendirilmiştir. Sonuçta %99,87 ve %99,78 ile DT ve RF algoritmaları en iyi sonuçları vermiştir. Ancak DT 4,53 sn hesaplama süresiyle RF algoritması 84,2 sn hesaplama süresinden daha iyi sonuç elde etmiştir.

Kumari ve Mrunalini (2022), DDoS ataklarının tespitinde önerdikleri matematiksel model ile makine öğrenmesi algoritmaları olan Lojistik Regresyon ve NB algoritmaları karşılaştırmıştır. Önerdikleri matematiksel model bant genişliği ve hedefe başarılı bir şekilde iletilen veri miktarı (verim) arasındaki olasılıksal ilişkiyi baz almaktadır. Çalışmada CAIDA 2007 veri seti kullanılmıştır. Deney sonuçlarında Lojistik Regresyon algoritmasında %99 ile %100 arasında, NB algoritmasında %99 ile %98 arasında doğruluk oranı elde etmişlerdir. Önerdikleri matematiksel modelde ise %99,75 oranında doğruluk değeri tespit edilmiştir.

Raj ve Kang (2022), DDoS ataklarının tespiti için makine öğrenmesi modeli geliştirmişlerdir. Geliştirilen model Lojistik Regresyon, SVM, XGBoost, DT, KNN makine öğrenmesi modelleri ile karşılaştırılmıştır. Çalışmada Mendeley’de bulunan Mininet veri seri üzerinde çalışma yapılmıştır. Sonuçlara göre XGBoost algoritmasında %98,38 doğruluk oranıyla en yüksek değer tespit edilmiştir.

Sharma ve Babbar (2023), DDoS ataklarını tespit etmek için ToN-IoT, CICDDoS2019 ve BoT-IoT veri setleri üzerinde KNN, NB, DT ve RF algoritmalarını kullanmıştır. ToN-IoT veri setinde KNN ve DT sırasıyla %98,8 ve %98 doğruluk oranı elde edilmiştir. CICDDoS2019 veri setinde DT ve RF algoritmalarının her ikisinde de %99 doğruluk oranı tespit edilmiştir. BoT-IoT veri setinde ise DT ve RF modellerinin her ikisinde de %100 doğruluk oranı tespit edilmiştir.

Avcı ve Koca (2023), bina otomasyon sistemleri üzerinde DDoS ataklarını tespit etmek için Yapay Sinir Ağı modelini ve SVM algoritmasını birleştiren yeni bir yöntem önermektedirler. Önerilen modelin sonuçları ile KNN algoritmasının sonuçları karşılaştırılmıştır. Geliştirilen algorithmada %99,19 oranında, KNN algoritmasında %96,46 oranında bir doğruluk değeri tespit edilmiştir. Çalışmada Kanada Siber Güvenlik Enstitüsü (CIC) IoT 2022 veri seti kullanılmıştır.

Kumar ve arkadaşları (2023), DDoS saldırılarını tespit etmek için Uzun Kısa Süreli Bellek (LSTM) tabanlı bir model oluşturmuşlardır. LSTM, özellik seçimi ve çıkarma algoritmasını içeren bir derin öğrenme yaklaşımıdır. LSTM eğitildikten sonra kendini güncelleme yeteneğine sahiptir. Çalışmada CICDDoS2019 veri seti kullanılmıştır. Deney sonuçlarında %98 oranında doğruluk tespit edilmiştir.

3. MATERYAL VE YÖNTEM

Bu bölümde yapılan çalışma kapsamında ön bilgiler derlenmiş ve sunulmuştur. Bilgisayar ağı kavramından, TCP/IP protokol kümesinden, ağ sistemleri için güvenlik kavramından, saldırı sistemlerinden, saldırı tespit sistemlerinden, DDoS atak türlerinden ve yöntemlerinden son olarak da DDoS atak tespiti ve sınıflandırılmasında kullanılan veri seti, veri seti ön işleme sürecinden ve makine öğrenmesi modelleri olan K-En Yakın Komşu, Rasgele Orman, Destek Vektör Makinası, Karar Ağaçları ve Naive Bayes algoritmaları anlatılmıştır.

3.1. Bilgisayar Ağı Nedir?

Bilgisayar ağı, temel olarak veri paylaşımı amacıyla çeşitli cihazları birbirine bağlayan bir teknolojidir. Farklı cihazlar arasında bilgi ve kaynak ihtiyacı, cihazların birbirine bağlandığı ağ adı verilen ve makineden makineye veri aktarımına olanak sağlayan bağlı bilgisayar sistemlerinin oluşturulmasına sebep olmuştur (Balcı, 2016). Meydana getirilen bu sistem ile makineler arasında iletişim gerçekleşir, data aktarımı yapılır ve ağda bulunan her türlü cihaz birbiri ile bağlantı kurabilir. Birçok farklı yöntemle bilgisayar ağı oluşturulabilir. Hepsinde ana amaç elde edilen bilgiyi paylaşmaktır. Bilgisayar ağı olarak isimlendirilen yapıya internete bağlanabilen her türlü cihaz dahil olur. Özellikle IoT ile birlikte ağa dahil olan makine sayısı orantısız olmayan bir hızla artmaktadır (Ma ve ark, 2023).

Bilgisayar ağına dahil olan cihazların birbirleriyle haberleşmesi için çeşitli protokoller oluşturulmuştur. İletişim kurmak için ağa dahil olan cihazlar, aralarında veri alış-verişini yapabilmek için ortak kurallar içeren protokoller zincirlerini kullanırlar (Mandle, 2001).

3.2. TCP/IP Protokol Kümesi

1969 yılında dört farklı yerdeki bilgisayarların birbirine bağlanması ile bilgisayar ağı oluşturulmuş ve ağa dahil olan cihazlar arası ortak iletişim sorunu ortaya çıkmıştır. Bu sorunu çözebilmek adına Açık Sistemler Ara Bağlantısı (Open Systems Interconnection-OSI) referans modeli Uluslararası Standart Ofisi (International Standart Office-ISO) tarafından 1984 yılında 7 katmanlı açık standart referans modeli olarak yayınlanmıştır. Ancak 1973'te Aktarma Kontrol Protokolü/İnternet Protokolü (Transmission Control Protokol/İnternet Protokol-TCP/IP) kümesi oluşturulmuştur ve internet bu model esas alınarak tasarlandığı için OSI referans modelinin kullanımı yaygınlaşamamıştır (Kırbaş, 2021).

TCP/IP protokol kümesi dört katmandan oluşmaktadır. Her katman birbirine hem hizmet sunar hem hizmet alır. TCP/IP protokol kümesi mimarisinde işlemler iki taraflı gerçekleşmektedir. Kullanıcı veriyi cihazın bağlı olduğu ağa gönderir ve sonucu cihazın bağlı olduğu ağdan alır. Bu işlemlerin gerçekleşmesi için mimari, katmanlar şeklinde tasarlanmıştır. TCP/IP protokol kümesinin birçok alt katman protokolü vardır ve bu protokoller IEEE tarafından geliştirilmektedir (Taner, 2017).

3.2.1. Ağ erişim katmanı

Bu katmanda pakete, paketin hangi sinyalle taşınacağı, bitlerin ne şekilde dizileceği, konnektörlerdeki kaç pin ile çalışılacağı, adaptörün ne zaman veri gönderip alacağı, teslimatın başarı durumu gibi detaylar tanımlanır ve pakete yazılır. Aynı zamanda fiziksel topoloji bu katmanda tasarlanır. OSI modelinde bulunan veri bağlantı katmanı ve fiziksel katmanın görevlerini yapar (Taner, 2017).

3.2.2. İnternet katmanı

Ağlar arasında veri iletimini sağlar. Veri iletiminin fiziksel ağlar arasında nasıl gerçekleşeceğini yönetir. İnternet katmanı adresleme ve yönlendirme, paketleme ve kapsülleme, fragmentasyon ve yeniden birleştirme, cihazlara IP adresinin atanması görevlerini yerine getirir. Bu katman iletişim kurulan ağın türüne bağlı olarak çeşitli protokollerle çalışır (Taner, 2017).

3.2.3. Taşıma katmanı

Birincil görevi, paketin alıcıya ulaştığından emin olmaktır. Uygulama katmanından gelen verileri, internet katmanının daha iyi anlayabileceği şekilde küçük parçalara böler. Bu parçalara segment adı verilir. Alt ve üst katmanların eş zamanlı çalışabilmesini sağlar. Bu işleme multiplexing adı verilir. Web’de gezerken aynı anda herhangi bir dosyanın indirilmesinden bu katman sorumludur. TCP ve UDP (Kullanıcı Veri Bloğu İletişim Kuralları-User Datagram Protocol) bu katmanda görev yapar (Taner, 2017).

3.2.4. Uygulama Katmanı

Bu katman insan makine iletişimin gerçekleştiği katmandır. OSI modelinde yer alan sunum katmanı, oturum katmanı ve uygulama katmanının işlevini TCP/IP modelinde uygulama

katmanı yerine getirmektedir. Uç düğümler arasında oturumun kurulmasını, yönetilmesini ve sonlandırılmasını gerçekleştirir. Kullanıcının isteklerini bilgi haline dönüştürerek karakter set çevrimi veya değiştirilmesi, şifreleme gibi görevleri yerine getirir. Farklı işletim sistemleri arasında ortak bir dil kullanımını sağlar (Taner, 2017).

3.3. Ağ Sisteminde Güvenlik Kavramı

Güvenlik, iç ve dış tehditlere karşı korunabilme yeteneği ve kapasitesidir (Kaypak, 2013). Güvenlik, nesnel olarak, kazanılmış değerlere yöneltilen tehditleri ölçmektir, öznel olarak ise bu değerlere saldırılacağı yönünde korkuların olmamasıdır (Aslanyürek, 2016). Güvenlik için verilen ödünleri tartışırken güvenliği sadece amaç olarak değil aynı zamanda bir sonuç olarak tanımlanması gerekmektedir. Güvenliğin ne olduğu veya ne kadar önemli olduğu güvenliği tanımlanan unsurları kaybetme tehdidi altında olmadan anlaşılmayabilir. Bu yüzden güvenlik tehditler aracılığıyla tanımlanır ve önemi anlaşılır (Ullman, 1983). Güvenliğin gizlilik, bütünlük ve erişebilirlik olmak üzere üç temel kriteri vardır. Gizlilik, korunan varlıklara sadece yetkili kişilerin erişmesi ve yetkisiz erişimlerin engellenmesidir. Bilginin gizlilik oranını, kimin bilgiye erişip erişmeyeceğini bilgiyi üreten belirler. Bütünlük, korunan varlıkların sahip olduğu tüm bileşenlerinin korunmasıdır. Bilginin ya da verinin herhangi bir şekilde değiştirilmesi, bozulması ya da silinmesi engellenmeye çalışılır. Erişebilirlik ise korunan varlıklara erişim yetkisi olan kişilerin istedikleri zaman erişebilmesidir. Herhangi bir şekilde erişimin kesilmesi erişilebilirlik özelliğini sağlamaz. Bu üç temel prensipten herhangi birinin eksik kalması durumunda güvenlik ihlali gerçekleşmiştir (Can ve Akbaş, 2014).

İnterneti meydana getiren şey bilgisayar ağlarının bir araya gelmesidir. Ağların güvenliği sağlandığı müddetçe internette sağlıklı bir veri alış-verişi olacaktır. İnternette güvenlik kavramını ilk defa Willis Ware 1967 yılında yayınladığı makalesinde ele almıştır. Ware'e göre dünyanın çeşitli coğrafyalarında bilgisayarlara erişim başlarsa, benzer kabiliyetlere sahip kullanıcılar ağdaki diğer cihazlara sızabilir. Ware aynı zamanda ABD Savunma Bakanlığı'nın bilgisayarlarında tutulan gizli projelerine, yabancı devlet ajanlarının da ulaşabileceğini varsaymıştır (Ware, 1967). İnternet yapısı bilgisayar ağlarının bir araya gelmesiyle oluşan bir sistem olduğu için güvenlik kavramı interneti oluşturan bütün birimleri kapsar (Kaya ve Öztürk, 2017).

Bilgisayar ağ güvenliği ise cihazların ve bağlı oldukları sistemlerin saldırganlara karşı korunmasıdır. Makinelerin dünyasında ağ güvenliği, bir bilgisayar veya ağ kaynaklarına yetkisiz erişimi, onların kötüye kullanımını, değiştirilmesini veya reddedilmesini önlemek,

tespit etmek ve izlemek için benimsenen politika, süreç ve uygulamalardan oluşan sistemdir. Cisco ağ güvenlik mühendisleri ise ağ güvenliğini ağın ve verilerin kullanılabilirliğini ve bütünlüğünü korumak için tasarlanmış herhangi bir etkinlik olarak nitelendirmiştir. Ağ güvenliğinin sağlanabilmesi için gizlilik, bütünlük ve erişilebilirlik özelliklerinin sağlanmasının yanında kimlik denetimi, izlenebilirlik ve inkâr edememe kriterlerinin de sağlanması gerekir. Kimlik denetimi, sisteme veya ağa erişmek için girişimde bulunan kişinin iddia ettiği kişi olduğunu kanıtlaması için gerekli olan aşamadır. İzlenebilirlik, sistemde veya ağ üzerinde gerçekleşen her türlü faaliyetin ve olayın daha sonra incelenebilmek için kaydedilmesidir. İnkâr edememe ise veri iletişimi esnasında veriyi gönderenin ve alanın, veriyi gönderdiğini ve aldığını inkâr edememesidir. Üretilen verinin üretildiği gerçeğinin değiştirilememesidir. Bu şartlardan herhangi birinin sağlanmaması sistemde ya da ağda güvenlik açıkları olduğu anlamına gelmektedir (Can ve Akbaş, 2014).

3.4. Saldırı Yöntemleri

Bilgisayar ağlarına ve sistemlerine karşı gerçekleştirilen saldırılar, illegal yöntemlerle hedeflenen bilgiyi ve veriyi ele geçirmek için gerçekleştirilen her türlü eylemdir (Hatipoğlu ve Tunacan, 2021). Siber saldırılar ağ modellemelerindeki zafiyetler, donanım ve yazılımdaki hatalar ve sistemlere online erişim imkanları sayesinde ortaya çıkmaktadır. Saldırganlar bu zafiyetleri kullanarak sistemlere erişim gerçekleştirir. Saldırıların amacına göre kurumlara, kişilere, devletlere yönelik birçok farklı boyutta gerçekleştirilebilir. Saldırganların amaçlarına göre kullandıkları saldırı yöntemi de değişiklik göstermektedir (Aslay, 2017). Literatürde yer alan bazı saldırı türleri aşağıda verilmiştir.

a) Bilgi ve veri aldatmacası (Data diddling)

Bilgisayara girişi yapılan verilerin hatalı girilmesi, verileri kayıt altına alırken değiştirilmesi ya da bazılarının silinmesi yöntemidir. Değiştirilen verilerin bilgisayar ortamında işlenmesi casuslar için hileli bir fayda sağlayabilir. Bazı durumlarda ise değiştirilen veriler işlendikten sonra tekrar orijinal haline döndürülerek etkinliğin gizli kalması amaçlanır. Bu saldırı yönteminin sonuçları çok büyük olabilir ve tüm sistemi kullanılamaz hale getirebilir (Wroblewski ve Hens, 1990).

b) Salam tekniği (Salami techniques)

Saldırganların genellikle finans sektöründe saldırı yapmak için oldukça yaygın kullandıkları bir metottur. Son derece küçük değişiklikler yapılarak gerçekleştirildiği için bu saldırıların fark edilmesi oldukça zordur. Örnek olarak bir banka muhasebecisi banka sunucularına her müşteri hesabından çok düşük miktarda nakit kesen bir program yerleştirir. Miktarın düşük olmasından dolayı müşterilerin çoğu bu kesintiyi fark etmeyebilir. Ancak muhasebeci her ay yüklü bir miktar nakit elde edebilir. Salam dilimleme (Salami Slicing) ve kuruş kesintisi (Penny Shaving) olarak bilinen iki farklı yöntemle gerçekleştirilir (Yazıcıoğlu, 2004).

c) Süper darbe (Super zapping)

Çoğunlukla her ağda sistem yönetici olarak bilinen ve sistemin herhangi bir yerindeki dosyaları okuma, silme ve oluşturma iznine sahip olan bir personel ya da bilgisayar programı vardır. Süper darbe ise sahip olunan bu ayrıcalıkların kötüye kullanılmasına verilen isimdir. Bu terim IBM tarafından geliştirilen ve ana bilgisayar yöneticilerinin sistemin herhangi bir yerinde olası bir arıza durumunda güvenlik önlemlerini geçersiz kılmasına olanak tanıyan yardımcı bir program olarak tasarlan Superzap programından türetilmiştir. Bu durumun sömürülmesi sonucunda saldırganlar güvenlik kontrollerine takılmadan sisteme sızarak süper darbe saldırısını gerçekleştirirler. (Turhan, 2006).

d) Truva atı

Truva atı olarak bilinen Trojan sistem içerisine hedeflenen bilgilere ulaşmak için ya da cihazı kendi çıkarları doğrultusunda kullanabilmek için özellikle yerleştirilen zararlı bir yazılımdır. Sisteme güvenli olmayan sitelerden video, dosya, fotoğraf vb. dosyaların indirilmesi ile bulaştırılabilir. Sisteme ulaştıktan sonra kendini hafızaya yükler ve saldırganın cihaza erişmesi için yetkisiz bir erişim noktası açarak kişisel ve finansal bilgilerin çalınması tasarlanır (Alkan, 2012).

e) Mantık bombaları (Logic bombs)

Bir yazılımın içeriğine belirli koşullar gerçekleşinceye kadar hareketsiz kalacak şekilde tasarlanarak yerleştirilen zararlı bir kod parçacığıdır. Tetiklendiğinde dosyaları silmek veya kritik sistemleri bozmak gibi yıkıcı aksiyonları gerçekleştirebilir. Birçok kötü yazılımın aksine aktif olarak yayılmazlar. Mantık bombası olarak adlandırılan kod parçacığının aktif olabilmesi

için genellikle belirli bir tarih ve saat, sistemde olması tahmin edilen bir durum, kullanıcı eylemleri, sistem koşulları tetikçi olarak işaretlenir. Tetiklenme koşulu gerçekleştikten sonra kod parçacığı çalışır. Amaç hedef alınan ağdaki ya da cihazlardaki verileri yok etmek ya da kullanılamaz hale getirmektir (Çelik, 2012).

f) Oltalama (Phishing)

Kişilere bilinen web sitelerinden ya da banka gibi resmi bir kurumlar tarafından gönderilmiş gibi gösterilen sahte elektronik postalarıdır (Yıldırım, 2018). Oltalama saldırıları genellikle bir kişinin kullanıcı hesap numaralarına, parolalarına, kredi kartı bilgilerine, banka hesap bilgileri gibi önemli bilgilere erişmek ve erişilen bu bilgileri satmak ya da kullanmak için gerçekleştirilir. Bu sahte elektronik posta içerisinde yer alan bağlantılarda genellikle virüs programları bulunmaktadır, böylelikle kişilerin özel bilgileri saldıran kişinin eline geçer. Kullanıcı bu durumu fark etmezse saldırganın tuzağına düşebilir (Aslay, 2017).

g) Bukalemun (Chamelon)

Zararsız güvenilir bir program gibi çalışır. Bir bukalemun yazılımı, yasal bir programı taklit ederek yazıldığında yasalar ile belirlenmiş yazılımların simülasyonu gibi görünürler. Ancak arka planda bir takım hile ve aldatmalar ile çok kullanıcıli sistemlerde kullanıcıların bilgilerini taklit ederek gizli bir dosyaya kaydedip, sistemin bakım için geçici bir süre kapatılacağına dair uyarı verir. Bu işlem gerçekleşirken bukalemun programını kullanan saldırgan kendi özel şifresi ile sisteme girer, kullanıcı bilgilerinin kaydedildiği gizli dosyaya erişerek kullanıcıların kişisel bilgilerini ele geçirir (Aydın, 1992).

h) Sistem güvenliğinin kırılıp içeri sızılması (Hacking)

Saldırganların hedef olarak seçtikleri sisteme yetkisiz erişim sağlamak için alışılmışın dışında, özgün bir tarzda sisteme sızmasıdır. Genellikle hedef sistemin güvenlik açıklarından yararlanarak, veri çalmak amacıyla gerçekleştirilen saldırı türüdür (Altınkaynak, 2017).

j) Port tarama (Port scanning)

Saldırganların ağdaki açık kapıları ya da zayıf noktaları bulmak için kullandıkları bir tekniktir. Saldırganlar hedef sisteme bir bağlantı göndererek her bir portu sırasıyla dener ve hangi portların cevap verdiğini not edip daha sonra bu portları analiz ederek sistemde güvenlik zafiyeti olup olmadığını tespit eder. Her açık port bir saldırgan için ağa sızabileceği savunmasız bir sistemin işaretçisidir. Port tarama saldırıları tek başlarına zararlı olmasa da saldırganlar

tarafından planlanan saldırının en önemli adımlarından biridir. Çünkü bu saldırılar sistemin zafiyetini bulup sömürmek için kullanmayı amaçlar (Altınkaynak, 2017).

k) Hizmet engelleme saldırıları (Denial of services)

DoS atakları teknik olarak saldırganın kurbanı tek bir kaynaktan tek bir hedefe saniye de milyonlarca veri paketi yollamasıyla gerçekleşir. Bu işlemle kurban üzerinde aşırı yüklenme oluşur ve legal kullanıcılar kurbanın verdiği hizmetlere erişemez (Gezgin ve Buluş, 2013). DoS ataklarında saldırganlar hedefe işleyişini engelleyen, kilitlenmesine, çökmesine, yeniden başlatılmasına veya gereksiz işler yapmasına neden olacak veri paketleri gönderir. Hedef sistemin güvenlik açıklıklarından yararlanarak ya da hedefin bant genişliğini, CPU, bellek gibi bazı önemli kaynakları tüketecek şekilde hazırlanmış veri paketlerini göndererek saldırı gerçekleştirilir. Bu durumda hedef sistem tüm kritik kaynaklarını saldırı trafiğini yönetmek için harcar ancak başaramaz ve hizmet dışı olarak görünür (Mirkovic ve ark, 2002).

l.) Dağıtık hizmet engelleme saldırıları (Distributed denial of services)

Temel olarak DoS saldırılarının gelişmiş versiyonudur. DoS saldırıları hedefe tek bir kaynaktan saldırı düzenlerken, DDoS ataklarında saldırganlar tarafından kontrol edilen BotNet ağı kullanılarak birden çok kaynaktan aynı anda hedefe saldırı gerçekleşir. İnternetin dizaynı gereği yapısından kaynaklanan açıklardan faydalanılarak, sistemin kaynaklarını tüketerek hizmet veremez hale getirmeyi amaçlayan saldırı türüdür. Bu saldırılar sürekli bir bilgisayar ya da bilgisayarlar tarafından sistem kilitleninceye kadar devam eder (Kaya ve Yıldız, 2014). DDoS saldırılarında hedefe meşru gibi görünen veri paketleri de gönderilmektedir ve saldırı paketi ile normal bir paketi ayırt etmek için çoğu zaman keskin bir belirti özelliği yoktur. Hedef sistem bir DDoS saldırısına maruz kaldığında sistem saldırıyı engelleyemez ve hizmet dışı olarak görünür (Mirkovic ve ark, 2002).

m) Yönetici hesabını ele geçirerek yerel ağda oturum açma (Remote to local-R2L)

Saldırganın kurban cihazda oturum açma izni olmadığı için bu cihazda yerel erişim elde etmek amacıyla cihazın bulunduğu ağ üzerinden cihaza güvenlik açığı varsa sömürmek için paketlerin gönderildiği saldırı türüdür. Saldırgan cihaza sızdıktan sonra kullanıcının bilgilerine erişir ve son kullanıcı olarak cihaz üzerinde ayrıcalıklar elde eder (Hassan, 2017).

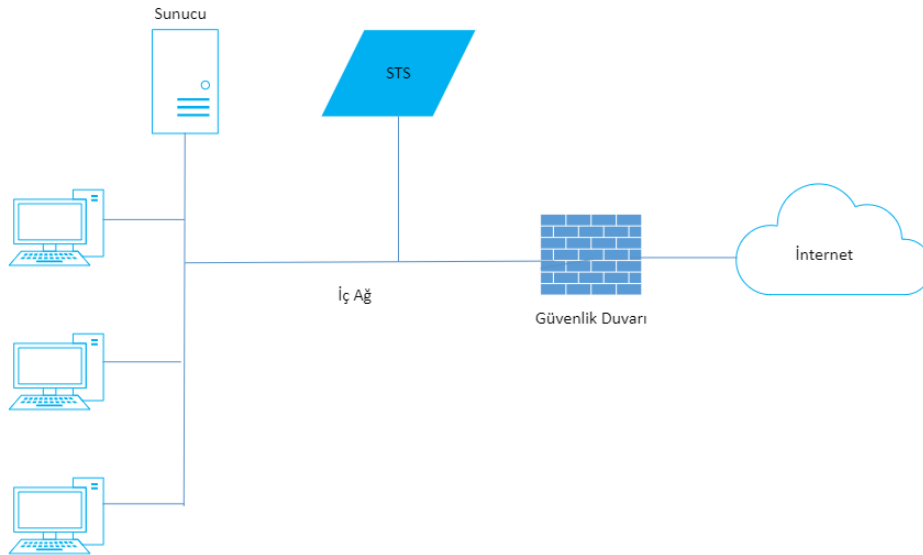
Sisteme erişebilen ancak yönetici yetkilerine sahip olmayan bir kullanıcının sistemin açıklarını kullanarak yönetici haklarını elde etmek için gerçekleşen saldırılarda kullanıcı

hesabını yönetici hesabına yükseltme (User to root-U2R) saldırıları olarak adlandırılmaktadır (Farid ve Rahman, 2010).

3.5. Saldırı Tespit Sistemleri (STS)

Bilgisayar ağı dünyasında ilk virüsler üretilip ağlara bırakılmaya, DoS atakları gerçekleşmeye, malware yazılımlarla sistemler çökmeye başladığında ağ teknolojileri için yeni bir boyut açılmıştır. 1967’de Ware’in öngördüğü gibi çok geçmeden, oluşturulan dünya çapındaki iletişim sistemi kötü niyetli kullanıcıların hedefi haline gelmiştir. Bu durumda ağ sisteminin korunması, ağların güvenli hale getirilmesi, kullanıcıların sistem içinde zarar görmemesi için ağ uzmanları tarafından güvenlik metotları geliştirilmeye başlanmıştır. Güvenlik duvarları, anti virüs yazılımları, cihazların işletim sistemlerini sürekli olarak güncel tutmak bu metotlar arasında yer almaktadır.

Saldırı tespit kavramı ilk olarak James Anderson tarafından 1980 yılında, bir makine sistemine zarar vererek kullanılamaz duruma getirmek ya da sisteme yetkisiz bir şekilde erişerek sistemdeki verilere ulaşmayı hedefleyen saldırı ve tehdit içeren olayların tespiti olarak tanımlanmıştır (Toprak, 2021). STS ağı dahil olan cihazlara karşı gerçekleştirilebilecek olası tehdit durumlarını anlamak için ağın gözetlenerek analiz edilmesi proseslerini içeren yapıdır (Sazzadul, 2012). STS’ler bir bilgisayar sisteminde ya da ağında meydana gelen olayları izleyen ve sistemin güvenliği için tehlike oluşturabilecek olası durumları analiz ederek ve sistem yöntemine bildiren cihaz ya da yazılım uygulamalarıdır (Scarfone ve Mell, 2007). Bace ve Mell saldırı tespit sistemini bilgisayar sistemine giren suçluları arayan, birilerini bu konu hakkında bilgilendiren ya da bilgisayar ve ağlar için hırsız alarmı olarak tanımlamıştır. Bace ve Mell STS’nin çalışma prensiplerini veri elde etme, çözümleme ve sonuç olarak üç bölümde ele almıştır. Veri elde etmek için sistemi tarayan ya da belirli konumlara yerleştirilmiş ajan adı verilen yazılım ya da donanım yapıları kullanılır. Çözümleme bölümünde ise tehdit olarak algılanan datanın sistemin kontrol mekanizmasından geçmesi işlemi gerçekleştirilir. Sonuç bölümünde ise datanın tehdit olup olmadığına karar verilip sitem yöneticisine bildirilir. Tehdit ise sistem alarm verir değil ise normal akışında devam eder. (Bace ve Mell, 2001). Şekil 3.1’de ağ tabanlı STS genel yapısı verilmiştir.

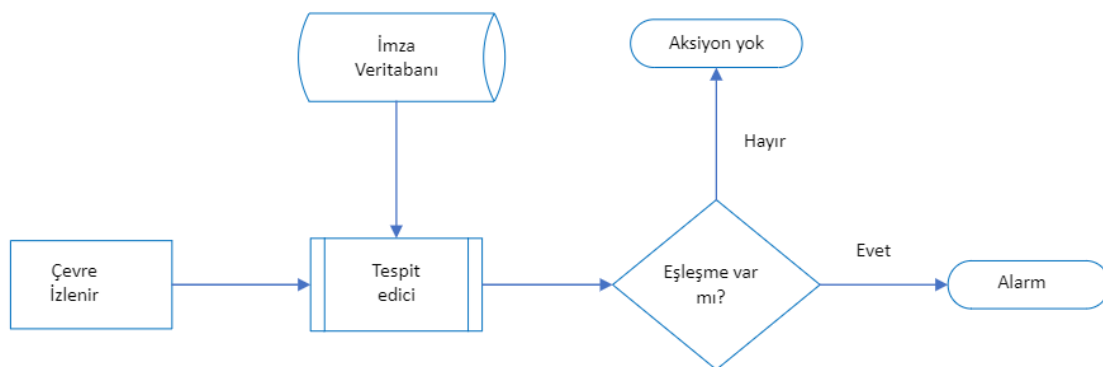


Şekil 3.1. Saldırı tespit sistemi genel yapısı

STS'ler genellikle güvenlik duvarı olarak nitelen özel ağın internet ile arasında yer alarak özel ağı koruyan sistem ile özel arasına yerleştirilir. Bu şekilde güvenlik duvarından geçen tehditlerin STS'ler aracılığıyla engellenmesi hedeflenerek sistem ve sistem içinde yer alan cihazlar korunur. Saldırı tespit metotları genel olarak üç ana başlık altında toplanır (Türkyılmaz ve Şentürk, 2022).

3.5.1. İmza tabanlı saldırı tespit yöntemi (Signature detection)

İmza tabanlı saldırı tespit yöntemi, olabilecek saldırıları belirlemek için sürekli güncellenen, önceden tespit edilmiş atak imzalarını ya da dijital ayak izlerini kullanır (Verma ve ark, 2018). İmza benzersiz bir tanımlayıcı olup saldırı için yazılan kod parçasının bayt dizisi olabilir. Belirli bir kalıpları olduğu için DNA ya da parmak izi gibi düşünülür. Şekil 3.2'de imza tabanlı saldırı tespit sistemi genel yapısı verilmiştir (Çil, 2021).

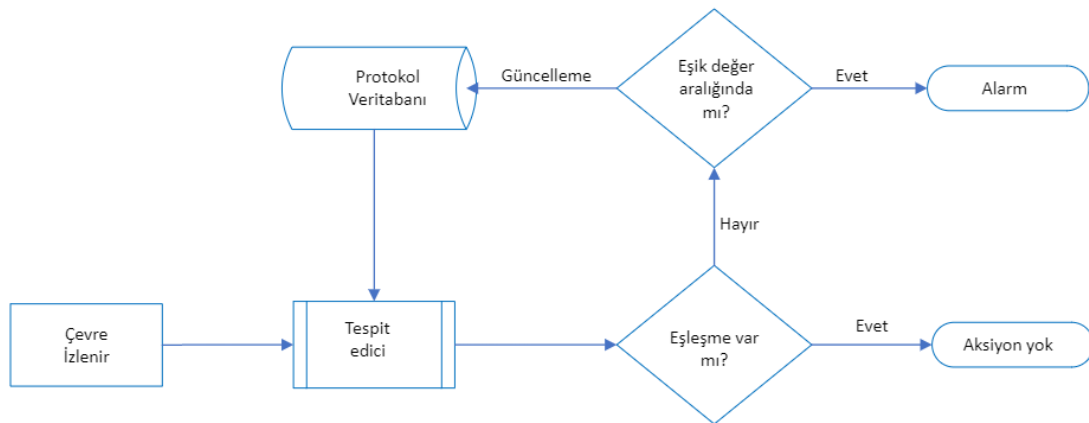


Şekil 3.2. İmza tabanlı saldırı tespit sistemi genel yapısı

Saldırı yapmak için tasarlanan her kötücül yazılımın imzası benzersizdir. Bu imzalar saldırıları tespit ederek analiz eden ve güvenlik açıklarını tespit eden araştırmacılar tarafından oluşturulur. İmza tabanlı saldırı tespit sistemlerinde bu imzalar STS kuralı olarak tanımlanır (Mudzingwa ve Agrawal, 2012). STS’lerde kural olarak tanımlanan bu imzalar veri tabanlarında depolanır. İzlenen ortamda veri tabanında bulunan imzalar ile eşleşen bir imza güvenlik saldırısı olarak işaretlenir ve sistem alarm verir. Karşılaşılan her yeni saldırıda imza niteliğindeki kod parçası sisteme eklenerek sistem güncellenir.

3.5.2. Anomali tabanlı saldırı tespit yöntemi (Anomaly detection)

Anomali tabanlı saldırı tespit sistemi gözlemlenen aksiyonu ağın ya da sistemin genel profili ile karşılaştırarak çalışır. Genel profil izlenen ağın ya da sistemin öğrenilen rutin davranış modeli olarak tanımlanır (Çil, 2021). İzlenen sistemin ya da ağın genel profili, anomali tabanlı STS’nin çevreyi izleyerek, sistemin rutin davranış kalıplarını analiz etmesiyle oluşturulur. Genel profiller dinamik ya da statik olabilir. Statik profiller bir kere oluşturulduktan sonra değişmez, dinamik profiller ise izlenen sistemlerin davranış modelleri değiştikçe güncellenirler. Bu profiller sistemin rutin aktivitesini tanımlamak için eşik değeri olarak kullanılır. Eğer sistemdeki veri akışı eşik değeri değerinden çok fazla sapma gösterirse uyarı verilir (Mudzingwa ve Agrawal, 2012). Şekil 3.3’te anomali tabanlı saldırı tespit sistemi genel yapısı verilmiştir (Çil, 2021).



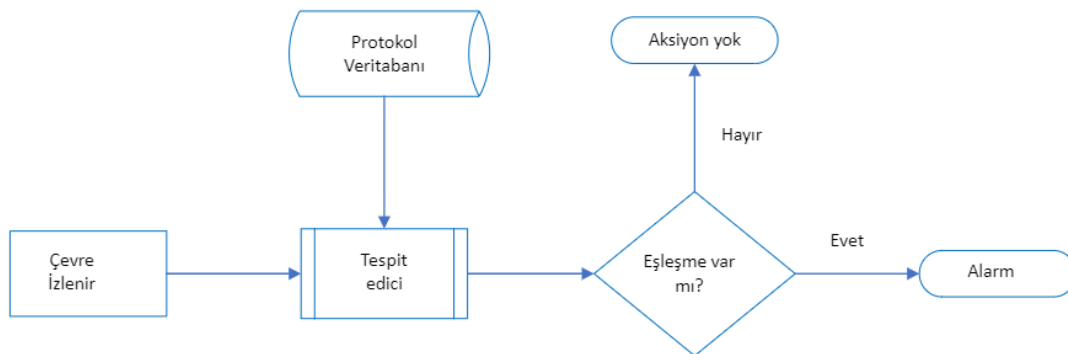
Şekil 3.3. Anomali tabanlı saldırı tespit sistemi genel yapısı

Anomali tabanlı STS’ler, sistemdeki anormal durumu tespit etmek için üç yöntem kullanır. Bu yöntemlerin ilki istatistiksel anomali tespiti, ikincisi veri madenciliği anomali tespiti ve üçüncüsü makine öğrenimi anomali tespitidir. İstatistiksel anomali tespit tekniğinde iki profil oluşturulur. Bu profillerden biri genel profil olarak nitelenir. Genel profil ağın

hareketlerinin uzun süreler içinde incelenmesi ile oluşturulan profildir. Diğerisi ise mevcut profil olarak nitelendirilir. Mevcut profil ağırlıklı hareketini temel alarak oluşturulan profildir. Eğer mevcut profil ile genel profil arasında herhangi bir farklılık var ise bu farklılık genel profilin eşik değeri aralığına göre anomali olarak işaretlenir. Anomali olarak işaretlendikten sonra sistem yöneticisine durum bildirilir. Veri madenciliği anomali tespit tekniği, anomali olarak görülen hareketleri otomatik bir şekilde tespit etmek için kullanılır ve bu işlemi yapabilmek için sistemi yüksek oranda dinlemeye alır. Bu dinleme sonuçlarına göre sistemdeki hareketlerin anomali olup olmadığı tespit edilir. Makine öğrenmesi anomali tespit tekniği ise sistem davranışlarını analiz ederek çalışır. Sistem genel davranışının eşik değeri hesaplanır. Sistemde var olan dataların eşik değeri hesaplanan eşik değeri aralığında ise herhangi bir sorun yok olarak algılanır, ancak eşik değeri aralığının dışında ise sistem durumu tehdit olarak algılanır ve alarm durumuna geçer (Mudzingwa ve Agrawal, 2012).

3.5.3. Durumsal protokol analizi saldırı tespit yöntemi (Protocol analysis)

Durumsal protokol analizi saldırı tespit yöntemi, saldırıları tespit etmek için her protokolün bilgisayar ağları çerçevesinde kabul görmüş standartlarına dayanan protokol modellerinin tanımlı olduğu veri tabanı, izlenen sistemlerdeki davranışları karşılaştırır. Durumsal protokol analizi STS'leri protokollerin nasıl kullanılması gerektiğini belirten geliştiriciler tarafından oluşturulan kuralları temel alır. STS ismi içinde yer alan "Durumsal" kavramı ağ, taşıma ve uygulama protokollerinin durumlarını izleme ve anlama yeteneği olarak tanımlanmıştır. Durumsal protokol analizi saldırı tespit yönteminde STS bir paket aldığı anda alıcı cihaz ile gönderici cihaz arasında bağlantı bilgileri, durum tablosu olarak nitelenen cihazlar arasındaki bağlantı kayıtlarını tutan listeye kaydedilir. Durum tablosunun içinde kaynak ve hedef IP adresi, port numaraları ve protokol bilgileri bulunur. Daha sonra bu bilgiler analiz edilir ve profile uygun düşmeyen paketlerin geçişi engellenir. (Scarfone ve Mell, 2007). Şekil 3.4'te durumsal protokol analizi tabanlı saldırı tespit sistemi genel yapısı verilmiştir (Çil, 2021).



Şekil 3.4. Durum protokol analizi tabanlı saldırı tespit sistemi genel yapısı

3.6. Saldırı Tespit Sistem Mimarileri

Teknolojinin hızla gelişmesiyle yeni yeni saldırı çeşitleri ortaya çıkmaktadır. Bu saldırıları tespit etmek için çeşitli STS mimarileri vardır (Koyuncu ve Ünlü, 2022). STS mimarileri çalışma prensiplerinde farklılık gösterse de hepsinde ortak olan temel bileşenler vardır. Bu bileşenler sensör, ajan, yönetim sunucusu, veri tabanı sunucusu ve konsoldur. Sensör genellikle ağ tabanlı, kablosuz ve ağ davranışı tabanlı mimarilerde ağı izlemek için kullanılan yapılardır. Ajanlar ise ana bilgisayar tabanlı mimarilerde sistemi izlemek için kullanılan yapılardır. Yönetim sunucusu sensörlerden ya da ajanlardan bilgileri alan ve bunları yöneten merkezi bir cihaz ya da yazılımdır. Veri tabanı sunucusu sensörler, ajanlar ve yönetim sunucusu tarafından kaydedilen durumların saklandığı depodur. Konsol ise STS kullanıcıları ve yöneticiler için arayüz sağlayan bir programdır (Scarfone ve Mell, 2007). STS mimarileri atak faaliyetlerini anlamak ve tanımlayabilmek için dört başlık altında incelenmektedir (Liao ve ark, 2013).

3.6.1. Ana bilgisayar tabanlı STS mimarisi (Host Based Intrusion Detection System-HIDS)

Ana Bilgisayar Tabanlı Saldırı Tespit Sistemi, genellikle hassas bilgiler içeren veya kamu ve özel sektörde kullanılan önemli alanlarda faaliyet gösteren ana bilgisayar sistemleri üzerine kurulan bir mimari içerir (Kurt ve ark, 2020). Ana bilgisayardaki sistem günlükleri, sistemin dahili bileşenleri ve ağdaki datalarla birlikte gözlemlenir ve analiz edilir. Bu mimari, bilgisayar ağlarındaki güvenlik tehditlerini tespit etmek ve incelemek için çeşitli teknolojileri ve algoritmaları bir araya getirir. Öncelikle sistem ağdaki trafiği izler. Bilgisayar ağındaki veri paketleri, log kayıtları ve diğer izlenen verileri toplar. Bu veriler ağın davranış biçimini tespit etmek ve trafiği analiz etmek için kullanılır. İzlenen ve analiz edilen verilere göre sistemin eşik değeri belirlenir ve bu aralığın dışında kalan her veri paketi tehdit olarak algılanır (Liao ve ark., 2013).

3.6.2. Ağ tabanlı STS mimarisi (Network Intrusion Detection System-NIDS)

Ağ Tabanlı Saldırı Tespit Sistemi ağı ya da ağda bulunan cihazları izler ve şüpheli etkinlikleri tanımlamak için ağ, taşıma, uygulama protokollerini analiz eder. Ağ tabanlı STS'ler de sensör, isteğe bağlı olarak bir veya daha fazla yönetim sunucu, konsol ve veri tabanı sunucusu bulunur. Sensörler tercihe bağlı olarak ya içinde sensör yazılımı yüklü olan bir cihaz olarak ya da sadece sensör yazılımı olarak sisteme entegre edilir. Sensörlerden gelen veriler

üzerinden yönetim sunucusu herhangi bir tehdit olup olmadığı analiz eder. (Scarfone ve Mell, 2007).

3.6.3. Kablosuz ağ tabanlı STS mimarisi (Wireless Intrusion Detection System-WIDS)

Yapısı itibarıyla NIDS ile benzerlik göstermektedir. Kablosuz sensör ağları ve kablosuz ağlar üzerindeki ağ trafiğini izler ve analiz eder (Liao ve ark, 2013). Ağ tabanlı STS'ler gibi kablosuz ağ tabanlı STS'lerde de sensör, isteğe bağlı olarak bir veya daha fazla yönetim sunucu, konsol ve veri tabanı sunucusu bulunur. Kablosuz ağ tabanlı STS'lerde ağ tabanlı STS'lerden farklı olarak izlenecek iki frekans (2,4 Ghz ve 5 Ghz) bandı vardır ve her bant kanallara ayrılmıştır. Bu teknolojiye bir sensörün bir banttaki tüm trafiği izlemesi henüz mümkün değildir ve bir sensör ancak bir kanalı izleyebilir. Sensör kanalı izlemeye hazır olduğunda kanal belirlenir ve sensör kendi radyosunu açar. Bu işlem sensörler arasında koordineli bir şekilde devam eder. Sensörler aracılığıyla izlenen ağdaki veriler yönetim sunucusuna aktarılır ve analiz edilir (Scarfone ve Mell, 2007).

3.6.4. Ağ davranışı temelli analiz mimarisi (Network Behavior Analise)

Ağ davranışı analizi kötü niyetli yazılım türlerini (solucanlar, Truva atı, malware, casus yazılımlar, virüs vb.), dağıtılmış hizmet reddi (DDoS) saldırılarını ve politika ihlalleri gibi ağda anormal örüntü meydana getiren durumları inceler. Diğer STS'ler gibi ağ davranışı temelli STS'lerde de sensör, isteğe bağlı olarak bir veya daha fazla yönetim sunucu, konsol ve veri tabanı sunucusu bulunur. Ağ davranışı temelli STS'ler de sensörler genellikle cihaz olarak bulunur. Sensörler ağdaki paketleri inceleyerek verileri yönetim sunucusuna aktarır herhangi bir tehdit olup olmadığı analiz edilir (Scarfone ve Mell, 2007).

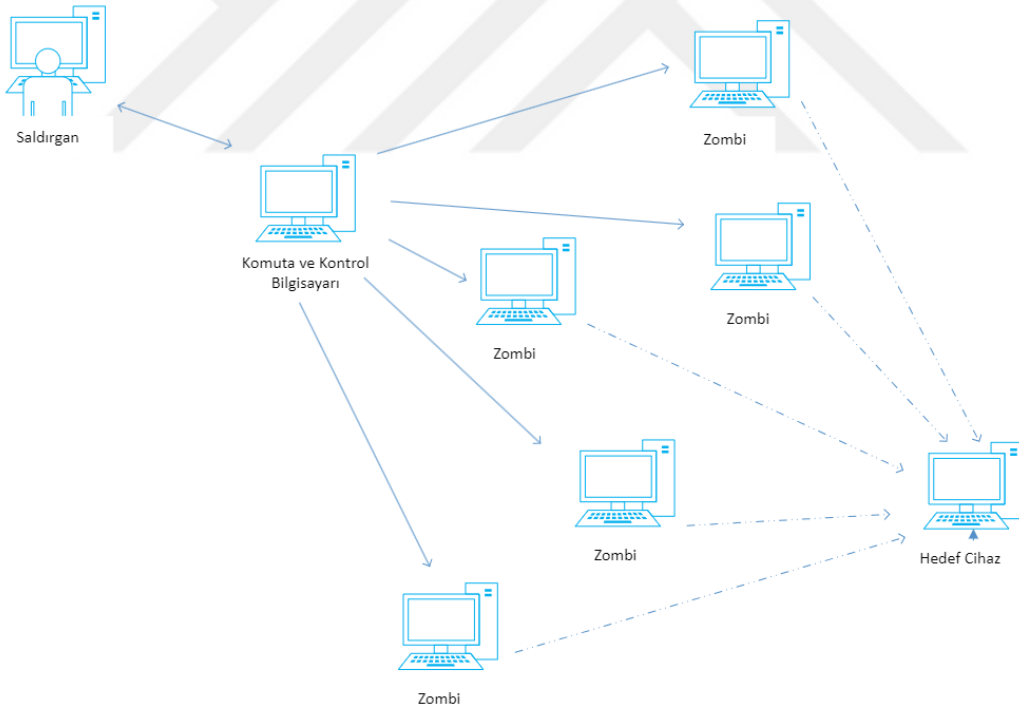
3.6.5. Derin öğrenme tabanlı mimari (Deep Learning Detection)

Derin öğrenme tabanlı analiz teknolojisinde makine öğrenmesi alt dallarından biri olan derin öğrenme modeliyle ağ trafiğinin küçük bir parçasından ağın genelinin profilini çıkarmak hedeflenir. Derin öğrenme temelinde var olan gizli katmanlar yardımıyla karmaşık veri kümelerinin özniteliklerini ve birbirleri arasındaki korelasyonu öğrenerek ağda bulunan saldırı paketlerini tespit etmesi saldırıları tespit etme sürecinde verimi arttırmaktadır (Viyanakumar ve ark, 2019). Bu yaklaşım tümevarım metodunu kullanarak diğer analiz metotlarına karşı avantaj oluşturur. Bu metodoloji iki kısımdan oluşur. İlk bölümde ağdaki data akışı kaydedilir, bu verilerle data seti oluşturulur ve derin öğrenme algoritması uygulanarak normal trafiğin profili

çıkarılır. İkinci bölümde is ağda ki mevcut paketler oluşturulan profil ile karşılaştırılır. Profile uymayan veriler sistemden düşürülerek bağlantısı kesilir (Doriguzzi ve ark, 2020).

3.7. Dağıtık Hizmet Aksatma (DDoS) Atağı Nedir?

Dağıtık Hizmet Aksatma atağı olarak tanımlanan bu kötücül yazılımlar kurban olarak seçilen sistemlerin çalışmasını sağlayan alt yapıların ve ağların hizmet verme kapasitelerinin üzerinde istek göndererek sistemin hizmet vermesini engellemeyi amaçlar. DoS ataklarının geliştirilmiş versiyonudur. DoS ataklarında tek bir kaynak cihaz kullanılırken DDoS ataklarında çeşitli zararlı yazılımlar aracılığıyla enfekte edilmiş zombi olarak adlandırılan birden çok cihaz kullanılır. DDoS atakları zombileştirdiği cihazları kullanarak, hedefin kaynaklarını tüketerek ya da ağın bant genişliğini potansiyelinin üstünde veri paketleriyle doldurarak hizmet reddi oluştururlar. Amaç hedef alınan sistemi işlevsiz hale getirerek erişiminin engellenmesidir (Khuphiran ve ark., 2018). Şekil 3.5'te DDoS saldırısı genel yapısı verilmiştir (Mirkovic ve ark, 2002).

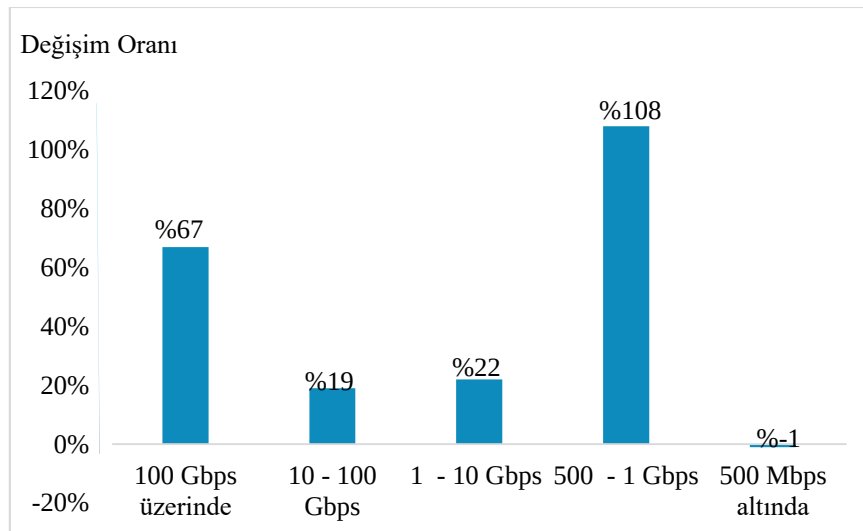


Şekil 3.5. DDoS saldırı genel yapısı

DDoS saldırılarının saldırganlar tarafından gerçekleştirilmesi için birkaç adım gerekmektedir. Bu adımlardan birincisi bir BotNet oluşturmak ya da kiralamaktır. Saldırıyı gerçekleştirecek olan kişi BotNet oluşturmak yerine kiralamak isterse yer altı dünyası olarak nitelenen camiadan kişilerle iletişime geçip BotNet kiralama ücretini ödeyerek BotNet kiralar.

Eğer saldırgan kendisi bir BotNet oluşturacaksa öncelikle güvenlik önlemlerinin yetersiz olduğu her türlü saldırıya açık cihazları tarayarak keşfeder. Tarama işlemi için çoğunlukla solucan yazılımları kullanılır. Solucanlar, bilgisayarları ve IoT cihazlarını enfekte eder. Bu cihazlar sadece saldırganın bulunduğu coğrafyadan değil dünyanın dört bir tarafından olabilir. Böylelikle saldırı gerçekleştikten sonra kendilerini koruma altına alırlar. Solucan yazılımlar IP adresinin 32 bitinin tamamı rasgele olacak şekilde ayarlayarak tüm interneti ayırım gözetmeden tarar ya da IP adresinin belirli kısımlarını ilk 8 veya 16 bitini rasgele olarak seçip tarama işlemini gerçekleştirebilir. Güvenlik açığına sahip cihazlara sızan solucanlar saldırganın sisteme erişmesi için arka kapı açar. Böylelikle saldırgan cihaza yönetim erişimi sağlar ve tespit edilen güvenlik açıklarını DDoS saldırısı yapmak için kullandığı DDoS yazılım setine dahil eder. Saldırı için kullanılacak cihazlar bulunduktan sonra bu cihazları koordineli bir şekilde hareket ettirebilmek ve kontrol edebilmek için aralarında iletişim kanalları kurarak kendi BotNet'ini oluşturur. BotNet'e dahil olan her bir cihaz zombi olarak isimlendirilir. Planlanan saldırının büyüklüğüne göre ağa dahil olan zombilerin sayısı artırılabilir. Saldırgan bu yapıda bir adet ya da ihtiyaca göre sayısını attırabileceği komuta ve kontrol (C&C) sunucusu/sunucuları oluşturur. Komuta ve kontrol cihazları ile zombi ağını kontrol ederek iş yükünü hafifletir. Saldırı gerçekleşeceği zaman saldırgan C&C sunucusuna komut verir ve ardından C&C sunucusu da zombi cihazlarını harekete geçirerek saldırıyı başlatır. Saldırı süresi ya saldırganın C&C sunucularına gönderdiği komutta belirtilir ya da manuel olarak ayarlanır.

Cloudflare tarafından yayınlanan 2022 DDoS atakları raporunda 2022 yılının son çeyreğinde gerçekleşen DDoS saldırılarında ani bir artış tespit edilmiştir. Şekil 3.6'da 2022 yılının son çeyreğinde DDoS ataklarının sayısındaki yüzdelik değişim grafik olarak verilmiştir (Anonim, 2022a).



Şekil 3.6. 2022 yılının son çeyreğinde DDoS ataklarının sayısındaki yüzdelik değişimi

Rapora göre 2022 yılının üçüncü çeyreğinden dördüncü çeyreğine;

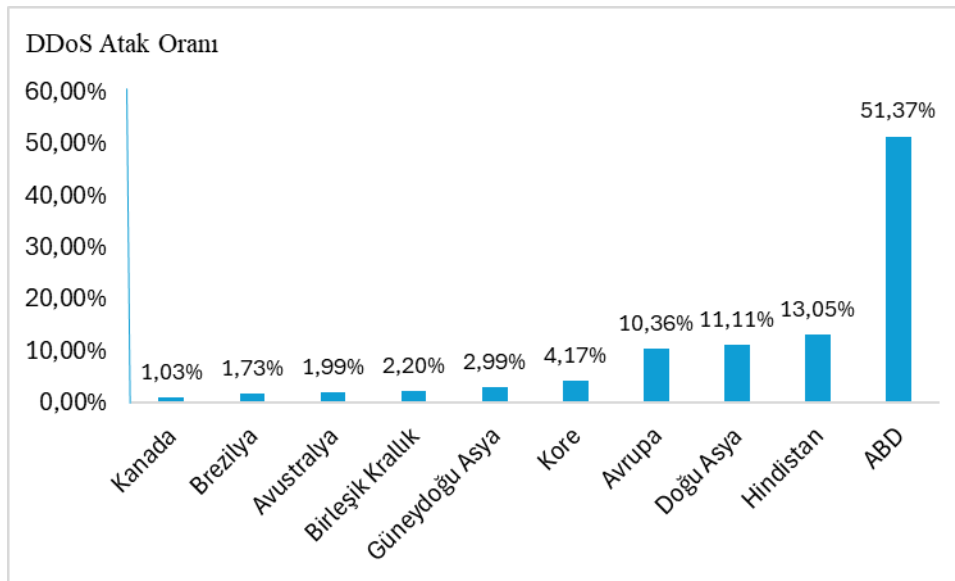
- ✓ Hızı 100 Gbps’yi aşan DDoS saldırılarının sayısı %67 oranında,
- ✓ Hızı 10 – 100 Gbps arasında olan saldırılar %19 oranında,
- ✓ Hızı 1 – 10 Gbps arasında olan saldırılar %22 oranında,
- ✓ Hızı 500 Mbps ile 1 Gbps arasında olan saldırılar %108 oranında

artış göstermiştir. Ancak hızı 500 Mbps’nin altında olan DDoS saldırılarında %1 oranında azalma meydana geldiği görülmüştür.

Çok yaygın olan bu saldırı çeşidinin yapılması çok kolaydır ve etkileri oldukça yıkıcı olabilir. Teknoloji ilerledikçe DDoS ataklarının hacmi de her geçen gün artmaktadır. Cisco tarafından yayınlanan Cisco Annual Internet Report (2018-2023) raporunda DDoS ataklarının 2018’de 7,9 milyon iken 2023’te iki katına çıkarak 15 milyonun üzerine çıkmıştır (Anonim, 2023a).

3.8. DDoS Atağı Örnekleri

Microsoft Azure’un yayınladığı rapora göre 2022 yılında saldırıların çoğu ABD merkezli kaynaklara yönelik gerçekleştirilmiştir. Diğer saldırıların büyük bir kısmı Hindistan, Doğu Asya ve Avrupa bölgelerini hedef almaktadır. Özellikle Asya’da akıllı telefonların giderek daha fazla kullanılması ve online oyunların cazibesinin artmasından dolayı DDoS ataklarına maruz kalma oranının arttığı değerlendirilmektedir. Bu durum sadece Asya ülkeleri için değil dijital dönüşümün hızla yol aldığı ve bulut teknolojisini benimseyen tüm ülkeler için geçerlidir. Şekil 3.7’de Microsoft Azure’un yayınladığı rapora göre ülkelere yönelik gerçekleşen DDoS atak oranları verilmiştir (Anonim, 2022b).



Şekil 3.7. Ünelere göre DDoS atakları

Rapora göre 2022 yılında DDoS saldırıları en yüksek oranda %51,37 ile ABD'ye yönelik, ardından %13,05 ile Hindistan'a yönelik gerçekleşmiştir. En az oranda %1,03 ile Kanada'ya yönelik gerçekleşmiştir.

Bilinen ilk DDoS atağı 1996 yılında en eski internet servis sağlayıcılarından biri olan Panix'i hedef alarak gerçekleştirilmiştir. DDoS saldırı türlerinden biri olan SYN seli saldırı metoduyla sistem birkaç gün boyunca hizmet dışı kalmıştır (Nicholson, 2022).

2016 yılının son çeyreğinde siber güvenlik uzmanı olan Brian Krebs'in bloğu saniye de 620 Gbps'yi aşan istek oranıyla DDoS saldırısına uğramıştır. Saldırının en önemli bileşeni Bir BotNet olan ve 600.000'den fazla güvenliği ihlal edilmiş IoT cihazından oluşan Mirai BotNet'tir (Warburton, 2021).

Mirai BotNet 2016 yılında ikinci saldırısı, bir milyondan fazla müşterisi için yaklaşık 18 milyon uygulamaya ev sahipliği yapan dünyanın en büyük veri merkezine sahip OVH'yi hedef almıştır. Tahmini 145.000 bot tarafından yönlendirilen, yaklaşık yedi gün süren saldırı saniyede yaklaşık 1.1 terabit trafik yükü oluşturmuştur (Warburton, 2021).

Mirai BotNet'in üçüncü saldırısı yine 2016 yılında gerçekleşmiştir. Ancak bu sefer bir fark vardır. Mirai yazılımı formlarda dağıtıldığı için mutasyona uğrayarak daha da güçlü hale gelmiştir. Bu gelişmeden sonra önemli bir DNS sağlayıcısı olan DYN'nin sunucuları, saldırganlar tarafından saniyede 1 terabit boyutunda taleplerle doldurulmuştur (Kochetkova, 2016). Saldırı ilerleyen zamanlarda saniye de 1.5 terabit hıza ulaşmıştır. DYN'nin hizmet veremez hale gelmiştir. Böylelikle GitHub, HBO, Twitter, Reddit, PayPal, Netflix ve Airbnb gibi bir dizi yüksek profilli web sitesini erişim kesintiye uğramıştır. Mirai BotNet bir DDoS saldırısının ne kadar da büyük çapta etki oluşturabileceğinin bir örneğidir. Mirai ağının boyutu ve karmaşıklığı, saldırıların ölçeği oldukça büyüktür (Warburton, 2021).

2018 yılının ilk çeyreğinde yazılım geliştiriciler için bir platform olan GitHub saniyede 1,35 terabit hızında ve yaklaşık 20 dakika süren bir DDoS saldırısına maruz kalmıştır. GitHub'a göre trafik on binlerce benzersiz uç noktada binden fazla farklı otonom tarafından düzenlenmiştir. Bu saldırı, web sitelerini ve ağları hızlandırmak için kullanılan Memcached sunucularının standart bir komutunun sömürülmesiyle gerçekleştirilmiştir. Cloudflare'nin raporlarına göre Memcached DDoS saldırı tekniği, 51.000 kata varan bir büyütmeye sebep olabilir. Yani 15 baytlık bir istek paketi ile 750 kb'lık yanıt alınabileceği anlamına gelmektedir (Warburton, 2021).

2020'nin son çeyreğinde 2020 ABD seçimleri nedeniyle Google hedef alınmıştır. Üç Çinli ISP'den gelen binlerce paketle Google IP adresine saldırı altı ay sürmüştür. Saniyedeki veri 2.5 Tbps ulaşarak rekor kırmıştır. Google Güvenlik Güvenilirliği Mühendisi olan Damian

Menscher saldırganın 167 Mpps (saniyede 167 milyon paket) ile CLDAP (Connection-less Lightweight Directory Access Protocol), DNS (Domain Name Server) ve SMTP (Simple Mail Transfer Protocol) sunucularına sahtekarlık yapmak için birkaç ağ kullanıldığını ve bu sunucuların Google IP'sine büyük yanıtlar gönderdiğini ifade etmiştir. Bu 2019'da rekor kıran Mirai BotNet'inin saniyede 623 Gbps olarak gerçekleşmiş saldırının dört katıdır (Warburton, 2021).

Amazon Web Services 2020 yılının Şubat ayında devasa bir DDoS saldırısına uğramıştır. Saldırganlar CLDAP protokolünü kullanarak kimliği belirsiz AWS (Amazon Web Service) müşterisini hedef almıştır. Bu saldırıda CLDAP sunucularından kurbanın IP adresine gönderilen veri miktarı 56 ila 70 kat arttırmıştır. Saldırı üç gün sürmüş ve saniyede 2.3 terabayta ulaşmıştır (Warburton, 2021).

Cloudflare 2023 yılı DDoS atakları raporuna göre, çevrimiçi saldırıların düzenli hedefi olarak da bilinen Kumar ve Oyun endüstrisi, 2023' ün 3. çeyreğinde en çok hedeflenen sektör olmuştur. İnternet ve Bilgi Teknolojileri sektörü ikinci sırada yer alırken onu Kripto Para sektörü izlemiştir (Anonim, 2023b).

2021'in 3. çeyreği, tarihteki en büyük HTTP (Hyper Text Transfer Protocol) DDoS saldırısını başlatmak için kullanılan en güçlü BotNet'lerden biri olan Meris BotNet'inin dönemi olmuştur. Finansal hizmetler sektöründeki bir müşteriyi hedef alan ve kaydedilen en büyük HTTP saldırılarından biri olan ve saniye 17,2 milyon rps (saniyede istek) istek oluşturan DDoS saldırısı gerçekleştirilmiştir. Şimdiye kadar gözlemlenen en güçlü BotNet'lerden biri olan Meris bu saldırıları başlatmak için kullanılmıştır. 2016 yılının Mirai BotNet'ine benzer şekilde Meris, kaydedilen en güçlü BotNet'lerden biri olmuştur (Warburton, 2021).

SOC (Security Operations Center) ekibinin istatistiklerine göre 2021 yılının ilk çeyreğinde gerçekleşen DDoS atağı oyun ve kumar organizasyonu için bilgi güvenliği hizmeti sağlayan A European Gambling Company'yi hedef alarak gerçekleşmiştir. Saldırı saniyede 800 Gbps veri akışı ile zirveye ulaşmıştır (Warburton, 2021).

CloudFlare'ın 2023 raporuna göre, dünya gündeminde yer alan bir diğer DDoS atağı örneği ise Orta Doğu ve Avrupa'da son zamanlarda yaşanan jeopolitik krizlerden hemen sonra başlamıştır. Rusya-Ukrayna savaşı ve akabinde vuku bulan İsrail-Filistin savaşı DDoS saldırılarının oranını arttırmıştır. Yayınlanan bu rapora göre en çok atak gerçekleştirilen sektör medya sektörü olmuştur (Anonim, 2023b).

3.9. DDoS Atak Yöntemleri

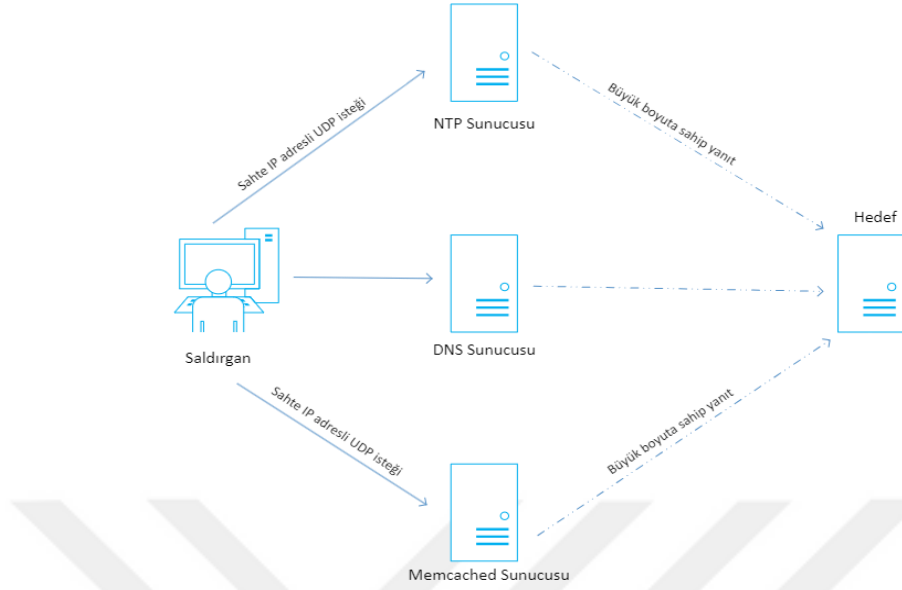
DDoS ataklarının temel felsefesi herhangi bir cihazın ya da sistemin sınırlılık içermesinden oluşmaktadır. Bilgisayarların, sunucuların, internet hatlarının belirli bir çalışma kapasitesi mevcuttur. Ve sınırlı kapasite sadece bilgisayar sistemlerinde bulunan cihazlar için değil var olan tüm sistemler için geçerlidir. Sistemler için sınırların ya da iş yükünün tanımını kullandığı amaç belirler. Bilgisayar sistemlerinde bu sınırlamaları donanım ve yazılım araçları belirlemektedir ve bu sistemler için iş yükü eş zamanlı kullanıcı sayısı, dosya boyutu, veri iletim hızı ya da depolanan veri miktarı gibi birçok bileşenle tanımlanabilir. Tanımlanan bu sınırların herhangi birinin aşılması sistemin çalışmasını engelleyecek ve hizmet dışı kalmasına sebep olacaktır (Şamlıoğlu, 2021). Bu bağlamda DDoS atakları kullandığı metotlara ve hedefe verdiği zarar yöntemlerine göre temelde Volümetrik, Protokol Katmanı, Uygulama Katmanı Saldırıları olmak üzere üç tipe ayrılmaktadır (Çil, 2021). Bu DDoS atak yöntemlerinde saldırganlar ağ trafiğinin yoğunluğunu attırmak için, hedefin sistemlerden istek talep ediyormuş gibi gösterildiği sahte IP adresleriyle ya da kötü amaçlı yazılımlarla içerisine sızılmış ve kontrol edilen cihazları kullanarak sahte trafik başlatırlar.

3.9.1. Volümetrik (Amplification) atakları

Volümetrik DDoS atakları hedef ile internet arasındaki bant genişliğini doldurmayı amaçlayarak hedefin hizmet dışı kalmasını sağlamaya çalışan DDoS atak yöntemidir (Shroff ve ark, 2022). Hedefe büyük ölçekte, kuvvetlendirilmiş ya da BotNet'ler üzerinden gelen milyonlarca veri paketiyle büyük bir trafik yönlendirerek internet bağlantısının sağlandığı ağ bant genişliği doldurulur. Bu durumdan ağa dahil olan tüm cihazlarda etkilenir ve ağ trafiği normal bir şekilde akış gerçekleştiremeyecektir (Şamlıoğlu, 2021). TCP/UDP Seli, ICMP Seli, NTP/Memcached kuvvetlendirmeli atakları volümetrik DDoS ataklarına örnektir. Saldırganlar, hizmet veren sunuculardaki DNS, NTP, Memcached gibi protokollerin zafiyetlerini sömürerek küçük boyutta gönderdiği paketleri çok büyük boyutlara ulaştırarak sistemi servis dışı bırakırlar (Altınkaynak, 2017).

Volümetrik DDoS atakları ağda tıkanıklığa odaklanmış gibi görünse de sistemlere sızma, daha karmaşık DDoS ataklarını kapsayan gizli bir amacında işaretçisi olabilir. Bu gibi durumlarda saldırganlar dikkatleri dağıtmak için mümkün olduğunca fazla operasyonel kesinti oluşturarak hedef şaşırtabilirler. Güvenlik ekipleri volümetrik saldırıyı azaltmak ya da önlemek için uğraşırken saldırganlar veri çalabilir, yüksek değerli hesaplara erişmeye çalışabilir ya da

ek saldırılar başlatabilirler (Şamlıoğlu, 2021). Şekil 3.8’de Volümetrik DDoS atak yapısı verilmiştir.



Şekil 3.8. Volümetrik DDoS atak yapısı

Volümetrik DDoS yapısına göre saldırgan erişebildiği sunuculara hedef sistemin IP adresini kullanarak istekte bulunur. Sunucular cevapları hedef sistemin IP adresine yönlendirerek sistemin bant genişliğinin kapasitesini ya da cihazın işlem kapasitesini doldurur. Böylelikle hedef sistemin hizmet dışı kalması hedeflenir.

3.9.2. Protokol atakları

İnternet üzerinden cihazların birbirleriyle iletişim kurabilmesi, veri alış-verişinde bulunması için çeşitli modeller geliştirilmiştir. Cihazların bir ağa dahil olarak birbirleri ile nasıl haberleşeceğine dair kurallar OSI referans modeli üzerinden tanımlanmıştır. Bu model Fiziksel Katman, Data-Link Katmanı, Ağ Katmanı, Transport Katmanı, Oturum Katmanı, Sunum Katmanı, Uygulama Katmanı olmak üzere yedi katmandan meydana gelir. Her bir katman içinde iletişimi kurmak için protokoller tanımlanmıştır (Çil,2021).

Protokol atakları internet iletişim protokollerinin zayıflıklarını temel alarak gerçekleştirilir. Bu protokollerin birçoğu küresel kullanımda devam ettiği için çalışma şekillerini yenilemek oldukça güçtür ve kullanıma sunulması ise çok yavaştır. Protokol DDoS atakları ağ katmanı ya da transport katmanı protokolleri üzerinden gerçekleştirilir. Amaç bu katmanlarda bulunan Güvenlik Duvarları, Yönlendiriciler, Yük Dengeleme Cihazları gibi ağ ve güvenlik cihazlarının yazılımsal ve donanımsal olarak kapasitelerini aşmasını sağlayarak

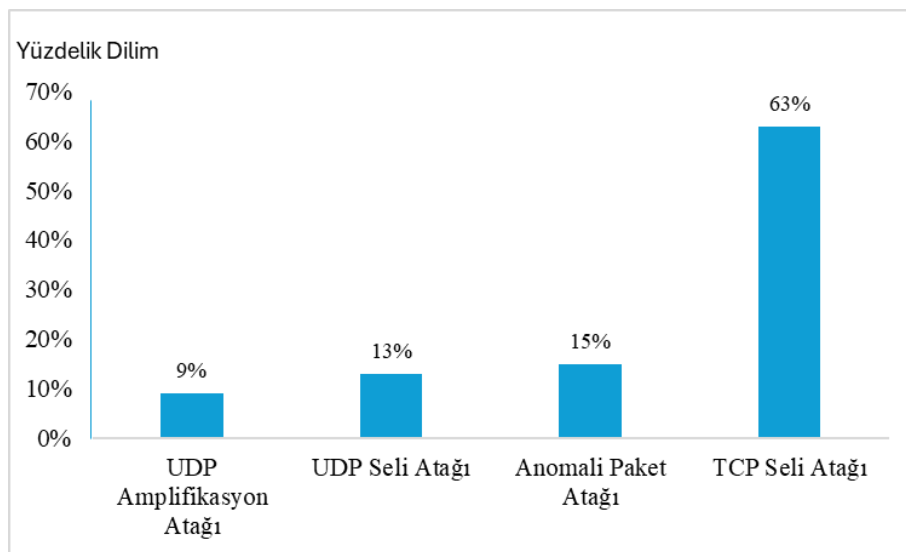
sistemin ve sistem elemanlarının devre dışı kalmasını sağlamaktır. SYN/SYN-ACK/ACK Seli, Smurf DDoS, Ping of Death atakları protokol ataklarına örnektir (Şamlıoğlu, 2021).

3.9.3. Uygulama katmanı atakları

Uygulama katmanı DDoS atakları hizmet reddi oluşturmak için hedefin kaynaklarını tüketmek üzerine kuruludur. Bu saldırılar uygulama katmanı içindeki güvenlik açıklarını kullanarak bu katmanda bulunan protokollere yönelik gerçekleştirilir. Uygulama katmanı saldırıları ağ bant genişliğini tüketmez, CPU döngüleri, veri tabanı döngülerini, bellek veya soket gibi bağlantı kaynaklarını tüketmeyi amaçlarlar. Bu katmana yönelik gerçekleşen DDoS atakları sunucuyu bozar bu nedenle daha az trafik olsa ve daha az bant genişliği kullanılsa bile sunucu çökebilir (Sunita ve ark, 2020). Uygulama katmanı ataklarında saldırı hedefindeki DNS, SMTP vb. web uygulama servislerine yanıtlayabileceğinden fazla isteklerle yanıt verme kapasitesini aşan paketler gönderilir. HTTP, HTTPS, SMTP ve DNS servislerine karşı gerçekleştirilen DDoS atakları uygulama katmanı ataklarına örnektir (Çil, 2021).

3.10. DDoS Atak Çeşitleri

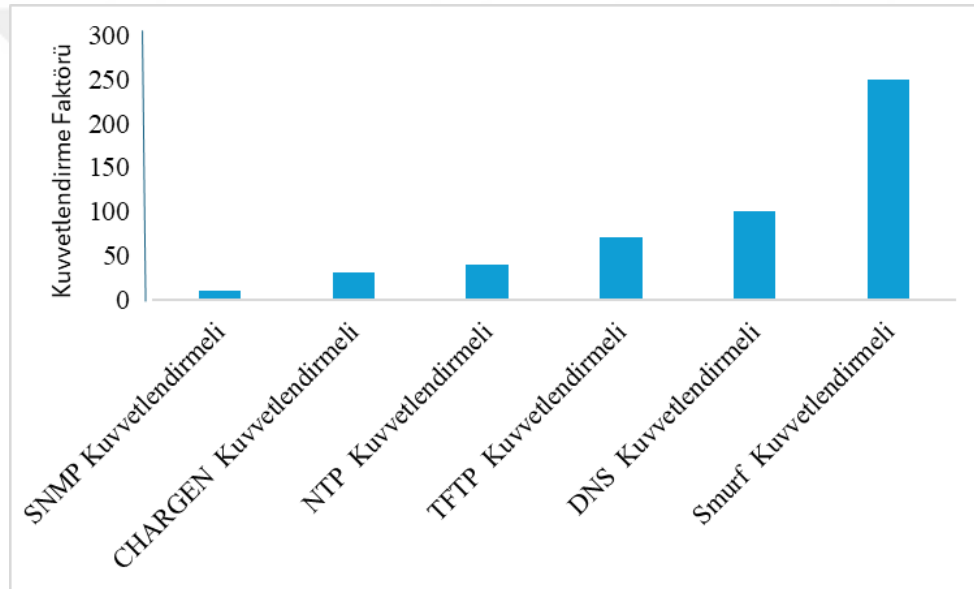
DDoS atak yöntemlerinin içinde flood (sel) atakları, yansıma atakları, amplifikasyon atak çeşitleri oldukça yaygın kullanılır. Flood ataklar hedefe aralıksız olarak istek gönderen ve BotNet'lerin yaygın olarak kullanıldığı DDoS atak çeşididir. SYN, UDP, ICMP, HTTP atakları bu tip ataklara örnek gösterilebilir (Altınkaynak, 2017). Şekil 3.9'da Microsoft Azure'un 2022 DDoS raporuna göre en çok gerçekleşen DDoS atakları verilmiştir (Anonim, 2022b).



Şekil 3.9. Microsoft Azure DDoS 2022 raporuna göre en çok gerçekleşen DDoS atakları

Microsoft Azure tarafından yayınlanan rapora göre 2022 yılında en çok gerçekleşen DDoS atak türü %63 ile TCP seli atağı olmuştur. En az gerçekleşen DDoS atak türü ise %9 oranında UDP amplifikasyon atakları olmuştur.

Amplifikasyon ataklarında saldırı küçük bir sorgu isteği ile başlatılıp hacimli yanıtların oluşturulmasıyla gerçekleşir. Bu tür ataklarda her çeşit sunucunun kullanılabilmesiyle saldırılar kuvvetlendirilir ve saldırıların etkisi arttırılır. Saldırganlar internette güvenlik açıklığı sebebiyle illegal olarak erişim sağlayabildikleri sunucuları kullanarak hedefledikleri sistemlere saldırı gerçekleştirirler. Bu sunucular aracılığıyla hedef sisteme gönderilecek paketlerin boyutunda büyütme gerçekleştirilerek sistemin kapasitesini aşmak amaçlanır. Şekil 3.10'da amplifikasyon DDoS ataklarının kuvvetlendirme faktörü verilmiştir (Sieklik ve ark, 2016).



Şekil 3.10. Amplifikasyon DDoS ataklarının kuvvetlendirme faktörü

DDoS ataklarının kuvvetlendirme faktörüne göre paketin boyutunda kuvvetlendirme faktörü ile Smurf ataklarında 250 kat, DNS ataklarında 100 kat, TFTP ataklarında 75 kat, NTP ataklarında 50 kat büyütme meydana gelebilir.

3.10.1. UDP seli atağı

Kullanıcı Datagram Protokolü (UDP) bağlantısız bir protokoldür. Veri paketleri UDP aracılığıyla gönderildiğinde, alıcı ile gönderici arasında herhangi bir anlaşma yapmaya gerek duyulmaz, alıcı sistem sadece işlenmesi gereken veri paketini alarak işlemleri gerçekleştirir. UDP veri paketini alan sistem belirtilen bağlantı noktasında UDP paketlerini almak için bekleyen bir program olup olmadığını kontrol eder. Paketleri almak için bekleyen bir program

var ise paketler işlenmek için alınır, eğer bekleyen bir program yoksa kaynak IP adresine ICMP hata mesajı gönderilir (Deshmukh ve Devadkar, 2015).

UDP'nin çalışma prensibini sömüren saldırganlar genellikle sahte IP adresleri kullanarak hedef sistemin belirli portlarına, rasgele olarak seçilmiş portlarına ya da tüm portlarına UDP paketleri gönderir. Sistem gelen UDP paketleri ortam dinlemesi yaptıktan sonra paketi alacak herhangi bir uygulama bulmaz ve kaynak IP adreslerine ICMP hata mesajları gönderir. Bu işlem saldırganın belirlediği zaman sürecince gerçekleşir ve hedef sistemin ağı UDP ve ICMP paketleriyle dolmaya başlar. Hedef sistemin ağ mimarisi ve hat hızına bağlı olarak işleyebileceğinden daha çok pakete maruz kaldığı için servis dışı kalır (Specht ve Lee, 2003).

3.10.2. SYN (Neptun) seli atağı

TCP iletişim protokolünü kullanarak gerçekleştirilen amplifikasyon DDoS atak çeşitlerinden biridir. Saldırganlar hedef sistemin kaynaklarını tüketerek meşru trafiğe kapatmayı amaçlarlar. TCP protokolünde bulunan “üçlü el sıkışma” metodundaki zayıflıktan yararlanılarak gerçekleştirilir. TCP ile gerçekleşen veri aktarımı bağlantılı odaklı olarak gerçekleşir. İki sistemin TCP ile bağlantı kurulabilmesi için “üçlü el sıkışma” prosedürünü yerine getirmesi gerekir. Bu prosedüre göre istemci sunucuya bağlantı kurmak istediğini belirtmek için SYN paketi gönderir. Sunucu aldığı SYN paketini doğrulamak için istemciye SYN-ACK paketi gönderir. SYN-ACK paketini alan istemci sunucuya ACK paketi gönderir ve iki sistem arasında bağlantı kurularak veri aktarımı gerçekleşir (Gürel ve Yalçinkaya, 2021).

SYN seli atağı ise TCP yapısında bulunan bağlantı kurma prensibinden yararlanarak gerçekleştirilir. Saldırgan bu saldırıyı ya kendi IP adresini kullanarak doğrudan ya da sahte IP adresleri kullanarak gerçekleştirir. Eğer saldırgan kendi IP adresini kullanırsa paket boyutunu çoğunlukla 64 byte olarak ayarlayıp hedef sisteme SYN paketlerini gönderir (Salunkhe ve ark, 2017). Hedef sistemden gelen SYN-ACK paketlerini ise yok sayarak ACK paketi göndermez ve sürekli SYN paketi göndermeye devam eder. Eğer sahte IP adresi kullanırsa hedef sisteme sahte IP adreslerini taklit ederek SYN paketleri gönderir ve hedef sistem bu IP adreslerine SYN-ACK paketleri gönderir. Her iki metotta üçlü el sıkışma işlemi gerçekleşmez. Bu durum hedef sistemde yarı açık bırakma etkisi oluşturur ve bu işlemin devamı için arabellekte yer ayrılmıştır. Ayrılan bu alan diğer servisler tarafından kullanılamaz ve yaklaşık üç dakika sonra bu bölgedeki paket bırakılır. Gelen her SYN paketi için tampon bölge ayrılır ve bir süre sonra limit dolar ve sistem yanıt veremez hale gelir. Her ne kadar SYN paketleri için ayrılan alanın süre

yaklaşık olarak üç dakika olsa bile saldırgan yüksek hızlarla SYN paketleri gönderdiği için sistemin kaynakları tükenir, yanıt veremez hale gelir ve servis dışı kalır (Şamlıoğlu, 2021).

3.10.3. ICMP seli atağı

ICMP protokolü ağ üzerinde bulunan cihazlar arası iletişim problemlerini teşhis etmek için kullanılan bir ağ katmanı protokolüdür (Gürel ve Yalçınkaya, 2021). ICMP protokolünün temel amacı hata raporlamasıdır. Alıcı ve gönderici arasında aktarılan verilerden herhangi birinin aktarımında aksama meydana geldiğinde ICMP protokolü ile hata mesajı iletilir. Bu protokolü kullanarak yazılan Ping programı cihazlar arası ağ bağlantısını test etmek, hedef cihazın veri aktarımı için açık olup olmadığını kontrol eder. Ping programı bu işlemi gerçekleştirirken ICMP istek mesajlarını kullanır. Hedef sisteme gönderilen ICMP istek mesajlarına, sistem açık ise ICMP cevap paketleri gönderir (Stiawan ve ark, 2021).

ICMP seli atakları ise protokolün çalışma prensiplerini kullanarak gerçekleşen bir DDoS saldırı türüdür. Saldırgan hedef sisteme Ping programı üzerinden ICMP istekleri göndererek sistemin gelen ve giden bant genişliğini tüketmeyi hedef alır ve çoğunlukla BotNet'ler üzerinden gerçekleştirir. Saldırgan tarafından ICMP istek paketlerini alan hedef sistem, ICMP cevap paketleriyle cevap verir. Bu şekilde bant genişliği tüketilerek sistem servis dışı kalır. Bu atak Ping programı üzerinden gerçekleştiği için ölümcül Ping atağı ya da Smurf atağı olarak da bilinmektedir (Gu ve Liu, 2012).

3.10.4. DNS kuvvetlendirmeli DDoS atağı

DNS kuvvetlendirmeli atakları DNS protokolünün kötü amaçlı kullanılması sonucu gerçekleşir. DNS protokolü insanların anlayabildiği karakterlerden oluşan alan adlarını cihazların anlayabileceği IP adreslerine çeviren bir sistemdir. Saldırganlar internetin en önemli bileşeni olan bu sistemi kullanarak hedef olarak seçtikleri sistemlere ataklar gerçekleştirirler (Altınkaynak, 2017).

Saldırgan DNS atağını gerçekleştirmek için öncelikle internette açık halde bulunan DNS çözümleyicileri tespit ederek güvenlik açıklarından yararlanarak sunucuyu manipüle ederler. DNS çözümleyiciler tespit edildikten sonra hedef sistemin IP adresi taklit edilerek bu sunuculara istekler atılır ve sunucularda isteklerin cevabını paket içinde yazan IP adreslerine gönderir. Bu şekilde hedef sistem DDoS saldırı altında kalır. Kuvvetlendirmeli DNS DDoS atağı ise DNS sorguları aracılığıyla yapılır. Kuvvetlendirme faktörü ise yanıt olarak gönderilen paket hacminin istek olarak gönderilen paket hacmine bölümüyle hesaplanır. Örneğin DNS

sorgu komutlarından biri olan ANY komutudur. ANY komutu, sorgusu yapılan alan adına dair tüm kayıt türlerini döndürmekle görevlidir. Bu bakımdan saldırgan ANY komutunu kullanarak belirtilen alan adıyla ilgili tüm kayıt türlerinin yer aldığı cevabı hedef sistemin IP adresine yönlendirerek DNS kuvvetlendirmeli DDoS atağı gerçekleştirir. Amplifikasyon saldırısında kullanılan bir diğer komut ise TXT komutudur. TXT komutu sorgulanan alan adının metinsel bilgilerini döndürür. TXT komutunun cevap içeriği de ANY komutu gibi büyük olduğu için DNS amplifikasyon DDoS ataklarında kullanılır. Ayrıca saldırgan BotNet kullandığı için hedef sistemin bant genişliği DNS yanıt paketleriyle dolarak ve hizmet reddi verir. (Rijswijk-Deji ve ark, 2014).

3.10.5. NTP kuvvetlendirmeli DDoS atağı

NTP, bilgisayar mimarilerinde saat senkronizasyonunu sağlayan bir protokoldür. NTP sunucuları cihazın saatini ayarlamak üzere cihazla 123 numaralı port üzerinden iletişim kurar. Bu atak çeşidini kullanan saldırganlar sahte IP'lerle NTP sunucusundan yapılan sorguları hedefe yönlterek ağın yük miktarını artırır (Çil, 2021). NTP sunucularında çalışan MONLIST komutu ile saldırganlar istek yaptıkları paketlere karşılık olarak cevap paketlerini büyütebilirler. MONLIST komutu NTP sunucularına istekte bulunan son 600 cihazın IP adresini tutmakla görevli bir komuttur. Bu özelliğinden ötürü saldırgan hedef sistemin IP adresini taklit ederek NTP sunucularına MONLIST komutu ile sorgu paketi yollar. Dönen cevap oldukça büyük kapasiteye sahip olur ve saldırgan bu işlemi sürekli tekrarladığı için hedef sistemin bant genişliği NTP paketleriyle dolmaya başlar ve hizmet reddi oluşur (Czyz ve ark, 2014).

3.10.6. SNMP kuvvetlendirmeli DDoS atağı

SNMP basit ağ yönetim protokolüdür. Ağa dahil olan tüm cihazların yönetimini, nasıl iletişim kurduğunu ve bilgi alışverişinde bulunduğunu tanımlar (Gürel ve Yalçınkaya, 2021). Yönetilen cihazların verileri Yönetim Bilgi Tabanı (MIB) adı verilen bir veri tabanında depolanır. Bu veri tabını cihazları izlemek ve eylemleri hakkında bilgi almak için kullanılır. SNMP protokolü içinde görev yapan GetBulkRequest komutu veri tabanı içinde birden fazla verinin bilgilerini aynı anda almaya yarayan bir yapıdadır. Bu komutun argümanlarından biri olan iterasyon sayısını “max repetitions” olarak ayarladığında maksimum sayıdaki veriyi döndürür. Bu şekilde saldırgan hacmi gönderdiği paket hacminden büyük olan bir yanıt paketini

hedef sisteme yönlendirilerek ANMP kuvvetlendirmeli DDoS atağını gerçekleştirir. (Gondim ve ark, 2020).

3.10.7. Character Generator Protocol (CharGEN) atağı

Character Generator Protocol (CharGEN), test ve performans ölçüm amaçları için kullanılan, 19 numaralı port üzerinden çalışan TCP/IP protokollerinden biridir. CharGEN protokolünün amacı yazıcıları test etmek ve bir sorun varsa sorunu gidermek için kullanılır. Hem TCP ile hem de UDP ile bağlantı kurarak çalışabilir. İstemci sunucudan karakter akışı oluşturmasını ve göndermesini CharGEN protokolü üzerinden ister. Saldırgan hedefe ait sahte IP adresiyle CharGEN protokolünün kullanıldığı birden fazla sunucuya istekte bulunur. İsteğe bulunan her bir sunucu hedef sistemin IP'sine büyük hacimli yanıtları gönderir. Cihazlar istekleri cevaplar ve hedef cihaza yoğun veri akışı olur. Sonuç olarak hizmet reddi oluşur (Gürel ve Yalçinkaya, 2021).

3.11. CICDDOS2019 Veri Seti

Bu çalışmada literatürde sıklıkla kullanılan CICDDOS2019 veri seti kullanılmıştır. CICDDOS2019, gerçek dünya verilerine benzeyen, iyi huylu ağ paketlerini ve en güncel DDoS ataklarını içermektedir. Veri seti oluşturulurken zaman damgasına, kaynak ve hedef IP'lere, kaynak ve hedef bağlantı noktalarına, protokollere ve saldırıya dayalı olarak etiketlenmiş akışlardan yeni öznitelik çıkaran CICFlowMeter-V3 kullanılmıştır (Sharafaldin ve ark., 2019). Veri setinde ataklar, yansımaya ve sömürü atakları olarak iki bölüme ayrılmıştır. CICDDOS2019 veri seti içinde yer alan yansımaya ve sömürü atak çeşitleri Çizelge 3.1'de verilmiştir.

Çizelge 3.1. CICDDOS2019 veri setinde bulunan DDoS atak çeşitleri

Yansımaya atakları		Sömürü atakları	
HTTP	SYN	UDP	UDP-LAG
MSSQL	SNMP	DNS	LDAP
SNMP	PORTMAP	NTP	TFTP

Yansımaya kaynaklı DDoS atakları, MSSQL Server, SSDP, NTP, TFTP, DNS, LDAP gibi yasal sunucuları kullanır. Sömürü kaynaklı DDoS atakları ise hangi protokolü kullanarak atak yapacak ise o protokolün zafiyetlerini kullanır. Çizelge 3.2'de CICDDOS2019 veri setinde bulunan bir paketin sahip olduğu öznitelikler verilmiştir.

Çizelge 3.2. CICDDOS2019 veri setinde yer alan bir paketin öznitelikleri

Öznitelik	Açıklama
Flow Duration	Akış süresi
Total Fwd Packet	İleri yönde toplam paket sayısı
Total Bwd Packets	Geri yönde toplam paket sayısı
Bwd Packet Length Max	Geri yönde maksimum paket boyutu
Bwd Packet Length Min	Geri yönde minimum paket boyutu
Bwd Packet Length Mean	Geri yönde paket boyut ortalaması
Total Length of Fwd Packet	İleri yönde toplam paket boyutu
Fwd Packet Length Max	İleri yönde maksimum paket boyutu
Fwd Packet Length Min	İleri yönde minimum paket boyutu
Fwd Packet Length Mean	İleri yönde paket boyut ortalaması
Flow IAT Max	İki akış arasındaki maksimum süre
Flow IAT Min	İki akış arasındaki minimum süre
Bwd Packet Length Std	Geri yönde paket boyutunun standart sapması
Flow Bytes/s	Byte'ın saniyedeki akış hızı
Flow Pakets/s	Paketin saniyedeki akış hızı
Flow IAT Mean	İki akış arasındaki ortalama süre
Fwd IAT Total	İleri yönde gönderilen iki paket arasındaki toplam süre
Fwd IAT Mean	İleri yönde gönderilen iki paket arasındaki ortalama süre
Fwd IAT Std	İleri yönde gönderilen iki paket arasındaki sürenin standart sapması
Fwd IAT Min	İleri yönde gönderilen iki paket arasındaki minimum süre
Fwd IAT Max	İleri yönde gönderilen iki paket arasındaki maksimum süre
Bwd IAT Mean	Geri yönde gönderilen iki paket arasındaki ortalama süre
Bwd IAT Total	Geri yönde gönderilen iki paket arasındaki toplam süre
Bwd IAT Max	Geri yönde gönderilen iki paket arasındaki maksimum süre
Fwd PSH Flags	İleri yönde hareket için PSH bayrağının kaç kez görüntülediği (UDP için 0)
Fwd URG Flags	İleri yönde hareket için URG bayrağının kaç kez görüntülediği (UDP için 0)
Bwd IAT Std	Geri yönde gönderilen iki paket arasındaki standart süre
Bwd IAT Min	Geri yönde gönderilen iki paket arasındaki minimum süre
Bwd PSH Flags	Geri yönde hareket için PSH bayrağının kaç kez görüntülediği (UDP için 0)
Bwd URG Flags	Geri yönde hareket için URG bayrağının kaç kez görüntülediği (UDP için 0)
Fwd Header Length	İleri yönde başlıklar için kullanılan toplam byte sayısı
Fwd Packets/s	Saniyede iletilen paket sayısı
Packet Length Min	Akışın minimum uzunluğu
Packet Length Mean	Akışın uzunluğunun ortalaması
Packet Length Variance	Paketin minimum varış süresi
SYN Flag Count	SYN paket sayısı
PSH Flag Count	PSH paket sayısı
URG Flag Count	URG paket sayısı
ECE Flag Count	ECE paket sayısı
Bwd Header Length	Geri yönde başlıklar için kullanılan toplam byte sayısı
Bwd Packets/s	Saniyedeki geriye dönük paket sayısı
Packet Length Max	Akışın maksimum uzunluğu
Packet Length Std	Akışın uzunluğunun standart sapması
FIN Flag Count	FIN paket sayısı
RST Flag Count	RST paket sayısı
ACK Flag Count	ACK paket sayısı
CWE Flag Count	CWE paket sayısı
Down/Up Ratio	İndirme ve yükleme oranı
Average Packet	Ortalama paket boyutu
Fwd Segment Size Avg	İleri yönde gözlemlenen ortalama boyut
Bwd Segment Size Avg	Geri yönde gözlemlenen ortalama boyut
Fwd Bytes/Bulk Avg	Ortalama byte sayısının ileri yönde toplu oranı
Fwd Packet/Bulk Avg	Ortalama paket sayısının ileri yönde toplu oranı
Fwd Bulk Rate Avg	İleri yöndeki toplu oranın ortalaması

Bwd Bytes/Bulk Avg	Ortalama byte sayısının geri yönde toplu oranı
Bwd Packet/Bulk Avg	Ortalama paket sayısının geri yönde toplu oranı
Bwd Bulk Rate Avg	Geri yöndeki toplu oranın ortalaması
Subflow Fwd Packets	İleri yönde bir alt akıştaki ortalama paket sayısı
Subflow Fwd Bytes	İleri yönde bir alt akıştaki ortalama byte sayısı
Subflow Bwd Packets	Geri yönde bir alt akıştaki ortalama paket sayısı
Subflow Bwd Bytes	Geri yönde bir alt akıştaki ortalama byte sayısı
Bwd Init Win Bytes	İlk pencerede geri yönde gönderilen bayt sayısı
Fwd Init Win Bytes	İlk pencerede ileri yönde gönderilen bayt sayısı
Fwd Seg Size Min	İleri yönde gözlemlenen minimum segment boyutu
Active Std	Bir akışın boşta kalmadan önce etkin olduğu standart sapma süresi
Fwd Act Data Packets	İleri yönde en az 1 bayt TCP veri yüküne sahip paketlerin sayısı
Active Min	Bir akışın boşta kalmadan önce etkin olduğu minimum süre
Idle Std	Bir akışın aktif hale gelmeden önce boşta kaldığı standart sapma süresi
Active Mean	Bir akışın boşta kalmadan önce etkin olduğu ortalama süre
Idle Min	Bir akışın aktif hale gelmeden önce boşta kaldığı minimum süre
Active Max	Bir akışın boşta kalmadan önce etkin olduğu maksimum süre
Idle Mean	Bir akışın aktif olmadan önce boş olması
Idle Max	Bir akışın aktif hale gelmeden önce boşta kaldığı maksimum süre

CICDDOS2019 veri setinin içinde bulunan toplam paket sayısı, iyi huylu paket sayısı, atak paket sayısı, deney çerçevesinde eğitim setinde kullanılan paket sayısı ve test setinde kullanılan paket sayısı Çizelge 3.3'te verilmiştir.

Çizelge 3.3. CICDDoS2019 veri seti dağılımı

Paket türü	Miktarı
İyi huylu paket sayısı	97831
Atak paket sayısı	333540
Eğitim seti paket sayısı	258822
Eğitim seti iyi huylu paket sayısı	58995
Eğitim seti atak paket sayısı	199827
Test seti paket sayısı	172529
Test seti iyi huylu paket sayısı	38836
Test seti atak paket sayısı	133713
Toplam paket sayısı	431371

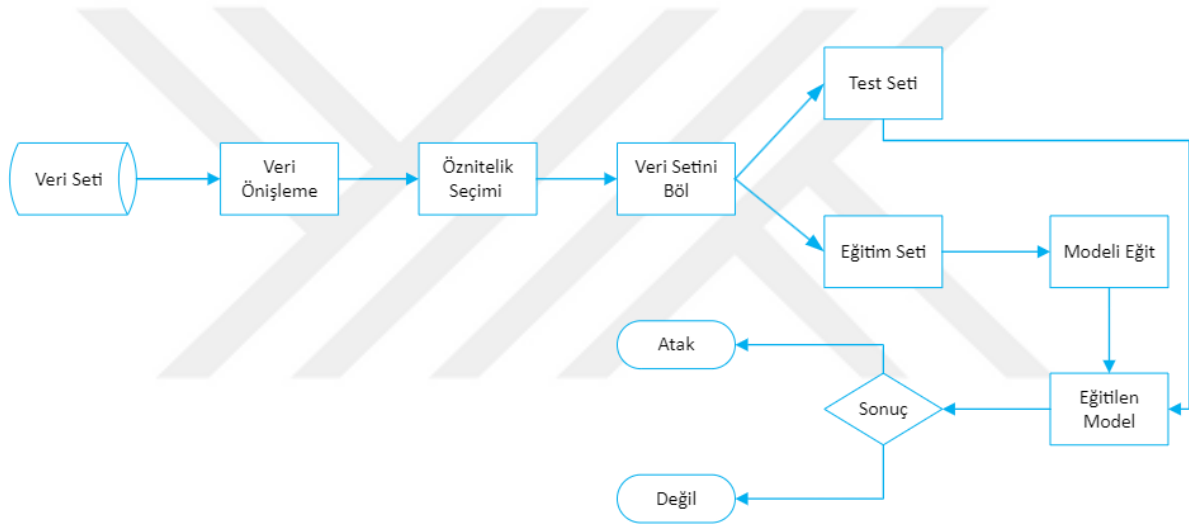
Çalışmada tespit edilmek üzere seçilen DDoS atak türlerinin eğitim seti ve test seti dağılımı Çizelge 3.4' te verilmiştir.

Çizelge 3.4. CICDDoS2019 veri seti DDos atak türleri dağılımı

DDoS Atak Türleri	Eğitim seti iyi huylu paket sayısı	Eğitim seti atak paket sayısı	Test seti iyi huylu paket sayısı	Test seti atak paket sayısı
LDAP	1173	257649	733	171816
UDP	10817	248005	7273	165276
MSSQL	248005	10817	3389	169160
NTP	72921	185901	48447	124102
DNS	2231	256591	1438	171111
SNMP	1644	257178	1073	171476
NETBIOS	383	258439	261	172288
TFTP	59076	199746	39841	132708
PORTMAP	367	258455	318	172231
WEBDDOS	32	258790	19	172530
SYN	29557	229265	19816	152733
UDP-LAG	35	258787	20	172529

3.12. Veri Önleme

Seçilen modellerin, veri seti üzerinde uygulamasına geçmeden önce çalışma amacına uygun olarak kullanılacak özniteliklerin seçilmesi gereklidir. Çünkü veri setinde bulunan tüm özniteliklerin kullanılması, uygulanacak her model için hesaplama maliyetini arttıracaktır. Bir diğer önemli faktör ise her bir özneliğin çıkış parametresine aynı önemde katkıda bulunmamasıdır. Bundan dolayı bilgi teorisi tabanlı, özniteliklerin bağımlı değişkenin belirlenmesindeki etkisini hesap eden Karşılıklı Bilgi (Mutual Information) yaklaşımı, çalışma kapsamında kullanılacak olan özniteliklerin seçimi için tercih edilmiştir (Çelik ve Bilge, 2015). Daha sonra içerisinde boşluk, gereksiz ve yanıltıcı bilgi bulunduran veriler tespit edilip, anlamlı hale getirilmiştir. Öznelik seçim işlemi tamamlandıktan sonra veri seti normalize edilmiştir. Çalışma kapsamında oluşturulan tespit mimarisi Şekil 3.11’de gösterilmektedir.



Şekil: 3.11. DDoS atak tespit mimarisi

3.12.1. Öznelik seçimi

Bilgi teorisi, bilginin ölçülmesi ve iletişimdeki etkisinin anlaşılması için matematiksel bir çerçeve sağlar. Bu teorinin önemli kavramlarından biri olan karşılıklı bilgi (KB), değişkenler arasındaki ilişkinin gücünü ve doğasını anlamak için ve değişkenler arasındaki ilişkiyi ölçmek ve bu ilişkinin sağladığı bilgiyi belirlemek için kullanılan bir ölçüdür. Bu yöntem değişkenler arasındaki bağıntıyı belirlerken, belirsizliği sayısal bir değere çevirebilen entropiyi ölçüt olarak kullanmaktadır (Estevez ve ark, 2013). Entropi, bir sistemdeki belirsizliğin veya karmaşıklığın sayısal ifadesidir. Bilgi teorisinde, entropi bir olasılık dağılımının belirsizliğini ifade etmek için kullanılmaktadır (Vergara ve Estevez, 2013). Çoğunlukla olasılık dağılımının entropisi Shannon entropisi olarak adlandırılır. Bilgiyi 0 ve 1 olarak matematiksel bir şablona dönüştüren Shannon’a göre entropi ne kadar küçük ise elde edeceğimiz bilgi o kadar kullanılabilir olur (Bahadır ve Türkmençalıkoğlu, 2021). Bu temel

üzerine kurulu olan Karşılıklı Bilgi metodu rasgele seçilen iki öznitelik arasındaki ilişkinin ölçüsüdür. Rasgele seçilen iki öznitelik arasındaki karşılıklı bilgi, bu değişkenlerin birbirlerine sağladığı bilginin derecesini ölçer. Ve bu bilgi ne kadar yüksek ise bu değişkenler arasındaki ilişki o kadar güçlüdür ve bu sonuçlar neticesinde verilerin sınıflandırılması ya da gruplandırılması için özniteliklerin belirlenmesi sınıflandırma işleminin doğruluğunun artmasına olanak sağlamaktadır (Learned-Miller, 2013).

Karşılıklı bilgi, bilgiyi ölçebilmek için değişkenlerin olasılık dağılımlarını kullanır. Denklem 3.1’de Karşılıklı Bilgi metodunun matematiksel formülü verilmiştir.

$$I(X; Y) = \sum_x \sum_y \left(P(x, y) \log \frac{P(x, y)}{P(x)P(y)} \right) \quad (3.1)$$

Bu denkleme göre;

x: Öznitelik kümesinden rasgele seçilen bir öznitelik (bağımsız değişken)

y: Sonuç kümesinden rasgele seçilen bir durum (bağımlı değişken)

I: Karşılıklı Bilgi

3.1’de verilen denkleme göre karşılıklı bilgiyi hesaplamak için bağımsız değişken kümesinden rasgele bir değişken seçilir. Ardından bağımlı değişken kümesinden rasgele bir durum seçilir. Seçilen bu iki durumun aynı anda olma olasılığı hesaplanır. Hesaplanan bu değer ile logaritma 2 tabanında seçilen değişkenlerin aynı anda olma olasılıklarının ayrı ayrı olma olasılıklarına oranın sonucu çarpılır. Bu işlem her öznitelik için gerçekleştirilir ve hangisinin karşılıklı bilgi sonucu yüksek ise o öznitelik sınıflandırma ya da yapılacak işlem için kullanılır (Estevez ve ark, 2013).

Rasgele seçilen özniteliklerin birbirleriyle olan ilişkisi hesaplandıktan sonra en büyüktен küçüğe doğru sıralanır. Veri seti üzerinde gerçekleştirilen ikili sınıflandırma işlemini yapmak için öznitelik seçme işleminde seçilen öznitelikler 78 öznitelik içerisinde en yüksek KB değerine sahip öznitelikler olarak belirlenmiştir. Bu öznitelikler Çizelge 3.5’te sunulmuştur.

Çizelge: 3.5. CICDDOS2019 veri seti ikili sınıflandırma öznitelikleri ‘Karşılıklı Bilgi’ değeri

DDoS atak türü	Seçilen öznitelik	KB değeri
UDP-LAG	Avg packet size	0.468842
	Packet length mean	0.434692
	Fwd packet length mean	0.433811
	Avg fwd segment size	0.433471
	Packet length max	0.424571
	Packet length min	0.420600
	Fwd packet length min	0.419849
	Fwd packet length max	0.416925
	Fwd packets length total	0.416769

	Subflow fwd bytes	0.415924
MSSQL	Fwd packet length min	0.080920
	Fwd packet length max	0.080616
	Packet length min	0.080568
	Packet length mean	0.077749
	Packet length max	0.076265
	Fwd packet length mean	0.075663
	Avg fwd segment size	0.075378
	Avg packet size	0.073433
	Fwd packet length total	0.066040
	Subflow fwd bytes	0.065626
LDAP	Protocol	0.058046
	Fwd packet length max	0.035291
	Fwd packet length min	0.030122
	Packet length min	0.029794
NTP	Fwd packet length max	0.598410
	Fwd packet length min	0.596968
	Packet length min	0.596734
	Packet length max	0.596229
	Fwd packet length total	0.594222
	Packet length mean	0.587429
	Avg fwd segment size	0.584250
	Fwd packet length mean	0.584241
	Avg packet size	0.582373
	Subflow fwd bytes	0.564878
DNS	Protocol	0.058345
	Fwd packet length max	0.044004
	Packet length min	0.040100
	Fwd packet length min	0.039964
SNMP	Protocol	0.058319
	Fwd packet length max	0.043822
	Packet length min	0.040597
UDP	Fwd packet length max	0.138023
	Fwd packet length min	0.133489
	Packet length min	0.133072
	Avg fwd segment size	0.131467
	Fwd packet length mean	0.131153
	Packet length mean	0.130809
	Packet length max	0.130771
	Avg packet size	0.125793
	Subflow fwd bytes	0.121684
	Fwd packets length total	0.121257
NETBIOS	Protocol	0.057539
	Fwd packet length max	0.024914
	Fwd packet length min	0.019250
TFTP	Fwd packet length max	0.550285
	Fwd packet length min	0.544568
	Packet length min	0.544375
	Fwd packet length mean	0.543133
	Avg fwd segment size	0.543115
	Packet length max	0.543021
	Packet length mean	0.542756

	Avg packet size	0.536164
	Fwd packets length total	0.525737
	Subflow fwd bytes	0.525591
PORTMAP	Protocol	0.057159
	Fwd packet length max	0.023160
	Packet length min	0.017408
WEBDDOS	Protocol	0.057024
	Fwd packet length max	0.017040
	Fwd packet length min	0.011230
SYN	Avg packet size	0.339400
	Flow bytes/s	0.319660
	Subflow fwd bytes	0.309594
	Fwd packet length total	0.309572
	Fwd packet length max	0.306145
	Packet length mean	0.304845
	Init fwd win bytes	0.304671
	Avg fwd segment size	0.302203
	Fwd packet length mean	0.301781
	Packet length max	0.298544

İkili sınıflandırma işleminde DDoS atak türlerinin tespiti için kullanılan öznitelikler;

- UDP-LAG DDoS ataklarının tespitinde ilk 10 öznitelikten sonra KB değerinde 0,3 değerinin altına düştüğü için ilk 10 öznitelik,
- MSSQL DDoS ataklarının tespitinde ilk 10 öznitelikten sonra KB değeri 0,05 değerinin altına düştüğü için ilk 10 öznitelik,
- LDAP DDoS ataklarının tespitinde ilk 4 öznitelikten sonra KB değeri 0,02 değerinin altına düştüğü için ilk 4 öznitelik,
- NTP DDoS ataklarının tespitinde ilk 10 öznitelikten sonra KB değeri 0,4 değerinin altına düştüğü için ilk 10 öznitelik,
- DNS DDoS ataklarının tespitinde ilk 4 öznitelikten sonra KB değeri 0,03 değerinin altına düştüğü için ilk 4 öznitelik,
- SNMP DDoS ataklarının tespitinde ilk 3 öznitelikten sonra KB değeri 0,03 değerinin altına düştüğü için ilk 3 öznitelik,
- UDP DDoS ataklarının tespitinde ilk 10 öznitelikten sonra KB değeri 0,11 değerinin altına düştüğü için ilk 10 öznitelik,
- NETBIOS DDoS ataklarının tespitinde ilk 3 öznitelikten sonra KB değeri 0,01 değerinin altına düştüğü için ilk 3 öznitelik,
- TFTP DDoS ataklarının tespitinde ilk 10 öznitelikten sonra KB değeri 0,4 değerinin altına düştüğü için ilk 10 öznitelik,

- PORTMAP DDoS ataklarının tespitinde ilk 3 öznitelikten sonra KB değeri 0,01 değerinin altına düştüğü için ilk 3 öznitelik,
- WEBDDOS DDoS ataklarının tespitinde ilk 3 öznitelikten sonra KB değeri 0,01 değerinin altına düştüğü için ilk 3 öznitelik,
- SYN DDoS ataklarının tespitinde ilk 10 öznitelikten sonra KB değeri 0,2 değerinin altına düştüğü için ilk 10 öznitelik tercih edilerek sınıflandırma işlemi yapılmıştır.

Çoklu sınıflandırma yapmak için kullanılan öznitelikler ise Çizelge 3.6’da sunulmuştur.

Bu sonuçlara göre veri setinde bulunan Çalışmada kullanılan öznitelik sayısı aşağıda verilmiştir.

Çizelge: 3.6. CICDDOS2019 veri seti çoklu sınıflandırma öznitelikleri ‘Karşılıklı Bilgi’ değeri

Sınıflandırma Türü	Seçilen öznitelik	KB değeri
Çoklu Sınıflandırma	Avg packet size	0.648207
	Packet length mean	0.613816
	Packet length max	0.608838
	Fwd packet length mean	0.607408
	Avg fwd segment size	0.607278
	Packet length min	0.603955
	Fwd Packet length min	0.602494
	Fwd Packet length max	0.598405
	Subflow fwd bytes	0.584867

Çoklu sınıflandırma işleminde ise ilk 9 öznitelikten sonra KB değeri %0,4’ün altına düştüğü için ilk 9 öznitelik tercih edilerek sınıflandırma işlemi yapılmıştır.

3.13. K En Yakın Komşu (KNN) Algoritması

KNN algoritması ilk olarak 1951’de Evelyn Fix ve Joseph Hodges tarafından geliştirilmiştir. İlerleyen dönemlerde Thomas Cover tarafından geliştirilerek parametrik olmayan bir sınıflandırma yöntemine dönüşmüştür. KNN algoritması aynı zamanda durum tabanlı akıl yürütme, örnek tabanlı akıl yürütme, hafıza temelli akıl yürütme ve tembel öğrenme olarak da adlandırılmaktadır. (Jabbar ve ark, 2013).

Danışmanlı makine öğrenmesi algoritmalarından biri olan KNN tüm durumları hafızasında tutup yeni durumları benzerlik ölçüsüne göre sınıflandıran, doğrusal olmayan bir yöntemdir (Jabbar ve ark, 2013). Sınıflandırılacak olan nesne en yakın kümeye dahil edilir. “k” burada pozitif bir tam sayı değeri ve özellikle tek tam sayı değeri almalıdır. Çünkü “k” değeri, algoritmada sınıflandırılacak olan vektörün tüm vektörlere olan uzaklıklarının hesaplanıp, bu değerlerin küçükten büyüğe doğru sıralandıktan sonra, hangi sınıfa dahil olacağını belirlemek için kullanılan bir parametredir. Dolayısıyla çift sayılarda sınıflandırmak için mevcut olarak

bulunan etiket gruplarının oranının eşit çıkma ihtimaline karşı alınan bir tedbirdir (Gürsaka, 2018).

“k” parametresi verilere bağlı olarak seçilir. Büyük k değeri gürültünün sınıflandırma üzerindeki etkisini azaltır ancak sınıfların sınırları daha az belirgin olur. Küçük k değerinde ise sınırlar oldukça net olur ancak gürültülü alanın etkisi artar.

Algoritmada k parametresi belirlendikten sonra sınıflandırılacak nesne ile diğerleri arasında uzaklık hesaplaması yapılır. Bu hesaplama;

- Euclidean (Öklit) Uzaklık hesaplaması,
- Manhattan Uzaklık Hesaplaması,
- Chebyshev Uzaklık Hesaplaması,
- Hamming Uzaklık Hesaplaması,
- Minkowski Uzaklık Hesaplaması,
- Mahalanobis Uzaklık Hesaplaması,
- Haversiense Uzaklık Hesaplaması,
- Levenshtein Uzaklık Hesaplaması,
- Sorensen-Dice Uzaklık Hesaplaması,
- Jaccard Uzaklık Hesaplaması

yöntemlerinden biri kullanılarak yapılır. Sonuçta sınıflandırılacak nesne en yakın olan kümeye dahil edilir (Fan ve ark., 2019).

Çalışma kapsamında yaygın olarak kullanılan Öklid uzaklık hesaplama yöntemi kullanılmıştır. Öklid uzaklığı, sınıflandırma ve kümeleme algoritmalarında sıklıkla kullanılan uzaklık ölçütüdür. Öklid uzaklığı, iki nokta arasındaki doğrusal uzaklık olup herhangi iki nokta, P ve Q arasındaki Öklid uzaklığı denklem 3.2 kullanılarak hesaplanır.

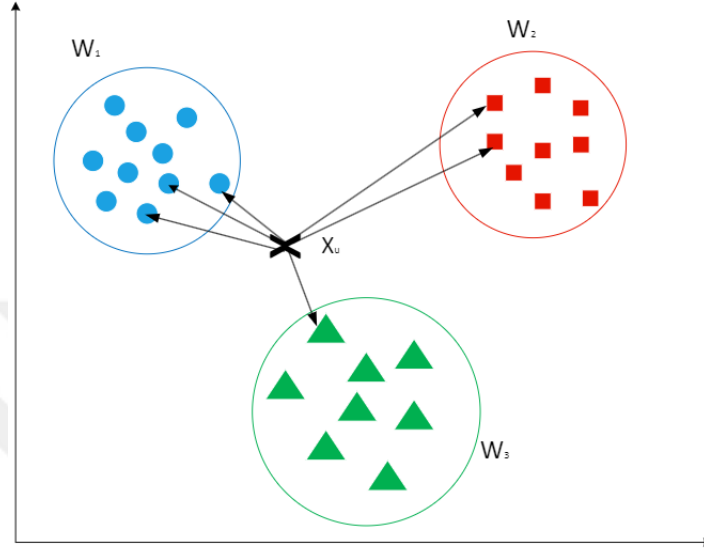
$$\sqrt{\sum_{i,j \in n} (x_i - x_j)^2 + (y_i - y_j)^2} \quad (3.2)$$

$$P = (x_1, x_2, \dots, x_n)$$

$$Q = (y_1, y_2, \dots, y_n)$$

P ve Q özniteliklerine sahip bir kümede Öklid bağıntısı 3.2’de verilen denklem ile hesaplanır. Seçilen verinin her bir özneliliğinin diğer tüm verilerin öznitelikleri ile arasındaki uzaklık hesaplanarak toplanır ve sonucun karekökü alınır. Daha sonra tüm hesaplanan değerler büyüktten küçüğe doğru sıralanır ve seçilen “k” değerine göre en baştan başlayarak, sınıflandırılmak istenen verinin hangi sınıfa dahil olacağı tahmin edilir.

Sonuç olarak KNN’de iki ana bileşen vardır. İlki nesneler arası uzaklık ikincisi ise k yakınlık noktasıdır. Bu iki bileşene göre KNN sınıflandırması yapılır. (Wang, 2019). Şekil 3.12’de KNN algoritması kullanılarak yapılan sınıflandırma işlemi gösterilmektedir (Fan ve ark., 2019).



Şekil: 3.12. KNN algoritması sınıflandırma işlemi

3.14. Naive Bayes (NB) Algoritması

18. yy’da matematikçi Thomas Bayes, Bayesyen yöntemlerin temelini oluşturacak Bayes teoremini ortaya atmıştır. Bayesyen bir yöntem olan Naive Bayes, danışmanlı makine öğrenme algoritmalarından biridir. KNN, Destek Vektör Makineleri ve Yapay Sinir Ağları yöntemleri gibi bir sınıflama kuralını doğrudan modellemez. Buna karşılık, Naive Bayes yöntemi sınıflandırma yaparken olasılıksal bir yaklaşım kullanır (Gürsaka, 2018).

NB basit fakat yüksek doğruluğa sahip bir sınıflandırma algoritmasıdır. Öznitelik seçiminde yüksek hassasiyete sahip olduğu için sınıflandırma yaparken doğruluğu etkileme dezavantajına sahiptir. (Putri ve ark, 2020). NB eğitim verilerinden yararlanarak öznitelik değerlerine göre her bir sınıf için gözlenen bir olasılık hesaplar ve daha sonra da bu gözlenen olasılıkları etiketlenmemiş test verileri üzerinde sınıfların tahmin edilmesinde kullanır. Bu algoritma verilerde eksik olduğunda veri temizleme işlemi yapılmadan da kullanılabilir olması bakımından avantaj sağlar (Rish, 2001).

Bayes teoreminin matematiksel formülü denklem 3.3’te verilmiştir.

$$P(c|x) = \frac{P(x|c)P(c)}{P(x)} \quad (3.3)$$

Burada;

c: Tahmin edilmeye çalışılan sınıf,

x: Sınıfı tahmin edilmek istenen durum,

$P(c|x)$: x durumu gerçekleştiğinde c sınıfının gerçekleşme olasılığı,

$P(x|c)$: c sınıfı gerçekleştiğinde x durumunun gerçekleşme olasılığı,

$P(c)$: c sınıfının gerçekleşme olasılığı,

$P(x)$: x durumunun gerçekleşme olasılığı,

Elde edilen bilgilerin artmasıyla birlikte herhangi bir durumu sınıflandırırken kullanılan özniteliklerin sayısı da artmıştır. Dolayısıyla NB sınıflandırılmasının temeli olan Bayes teoreminin denklemi de özniteliklerin çokluğu dikkate alınarak zincir kuralına dayanarak genişletilmiştir. Bu kurala göre;

$x=(x_1, x_2, x_3, \dots, x_n)$ özniteliklerini temsil eden küme ise;

NB algoritmasında kullanılan matematiksel denklem 3.4 olarak güncellenir.

$$P(c|x_1, x_2, x_3, \dots, x_n) = \frac{P(x_1|c)P(x_2|c)P(x_3|c) \dots P(x_n|c)P(c)}{P(x_1)P(x_2)P(x_3) \dots P(x_n)} \quad (3.4)$$

3.4'teki denklemin paydası tüm özniteliklerde aynı olduğu için sabit kalır ve bu nedenden dolayı denklemden kaldırılır ve düz orantı bağıntısı kullanılır. Sonuçta yeni denklem 3.5 olur. Elde edilen bu denklemde maksimum olasılık sonucunu veren sınıf gruplandırılmak istenen nesnenin sınıfı olarak işaretlenir (Wickramasinghe ve Kalutarage, 2021) .

$$P(c|x_1, x_2, x_3, \dots, x_n) = P(c) \prod_{i=1}^n P(x_i|c) \quad (3.5)$$

NB yönteminde temelde iki varsayım vardır. Biri tüm sınıfların istatistiksel olarak birbirinden bağımsız olmasıdır, ikincisi ise tüm sınıfların hedef sınıfa katkıda bulunması ve katkılarının eşit olmasıdır. Bu yöntemde model bir kere eğitildikten sonra yüksek performanslı çalışır. Sonuç olarak Bayes yöntemi sınıflandırma yaparken hedef sınıfın değerlerinin gerçekleşme olasılığına göre hareket eder (Rish, 2001) .

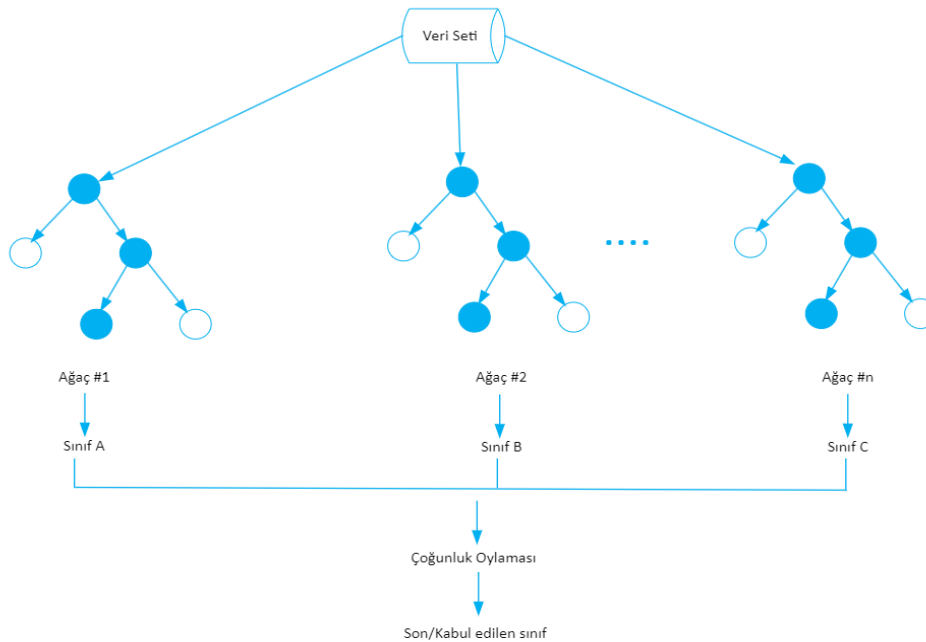
3.15. Rasgele Orman (RF) Algoritması

Rasgele Orman, Leo Breiman ve Adele Cutler'in geliştirdiği ve sonuca ulaşmak için birden çok karar ağacının sonuçları arasında oylama yöntemi kullanılarak en çok oy olan sınıfın tercih edildiği, yaygın olarak kullanılan bir sınıflandırma algoritmasıdır. Toplu sınıflandırma

yöntemlerinden biri olan RF algoritması, bir sınıflandırıcı yerine birden çok sınıflandırıcı üretir ve daha sonra oy kullanma yöntemi ile en çok oy alan sınıfa sınıflandırılmak istenen veriyi ekler. Hızlı olması, aşırı uyuma karşı dayanıklı olması ve ağaç sayısının belirlenebiliyor olması RF algoritmasını ayrıcalıklı hale getiren nitelikleridir (Breiman, 2001).

RF algoritması, rastgelelik özelliği eklenerek diğer bir toplu sınıflandırma algoritması olan Torbalama (Bagging) metodunun geliştirilmiş halidir (Breiman, 2001). Karar ağaçlarındaki gibi tüm değişkenler içinde en iyi dalı seçerek her bir düğümü dallara ayırmak yerine, her bir düğüm için rastgele olarak seçilen nitelikler içinden en iyisi kullanarak dallandırmayı gerçekleştirir. Oluşturulan her bir veri seti ana veri setinden seçmeli olarak üretilir. Bu işlemden sonra rastgele özellik seçimiyle ağaçlar oluşturulur. Oluşturulan bu ağaçların hiçbirisi budanmaz (Archer ve Kimes, 2008).

RF algoritması, eğitimden önce ayarlanması gereken üç ana parametreye sahiptir. Bunlar, düğüm boyutunu, ağaç sayısını ve örneklenen özelliklerin sayısını içerir. Topluluktaki her ağaç, önyükleme seti adı verilen eğitim kümesinden alınan bir veri setinden oluşur. Bu eğitim örneğinin üçte biri test verileri olarak ayrılır. Daha sonra, veri kümesine daha fazla çeşitlilik ekleyerek karar ağaçları arasındaki korelasyon azaltılır. Özelliğe torbalama yoluyla başka bir rastgele veri enjekte edilir. Sınıflandırma görevi için çoğunluk oyu- yani en sık görülen kategorik değişken- tahmin edilen sınıfı belirler. Sonuç olarak Rasgele Orman algoritması çoklu karar ağaçlarının sonuçlarının en iyiye doğru sömürülmesi yöntemiyle çalışan etkili bir makine öğrenmesi yöntemidir. Şekil 3.13'te RF algoritması kullanılarak yapılan sınıflandırma işlemi gösterilmektedir.

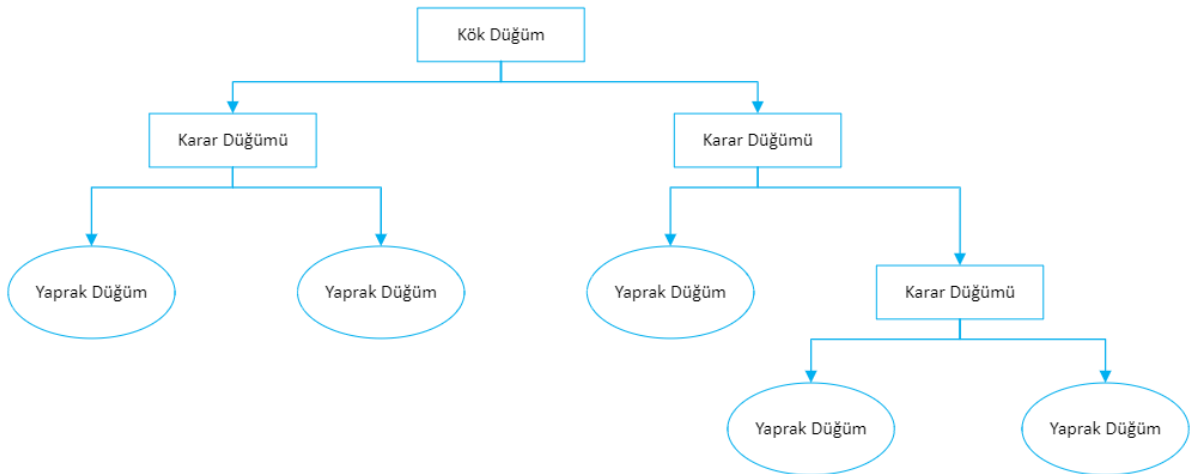


Şekil 3.13. RF algoritması sınıflandırma işlemi

Bu çalışma kapsamında RF algoritmasında eğitim aşamasında hangi öznelik üzerinden bölme işleminin gerçekleşeceğini belirlemek için eşitlik 3.6, 3.7 ve 3.8’de verilen GINI indeksi kullanılmıştır. Bir düğüm için GINI indeksinde önemli bir azalma meydana gelmiyorsa düğüm terminal düğüm olarak belirlenir (Çelik ve ark., 2018). Terminal düğümün sınıfı, çoklu oy kuralına göre belirlenir (Breiman ve ark, 1984).

3.16. Karar Ağacı Algoritması (DT)

Karar ağacı, sınıflandırma ve regresyon problemlerini çözmeye elverişli, danışmanlı bir yapay zekâ algoritmasıdır. Karar ağaçlarında verinin sınıflanması öğrenme ve sınıflama bölümlerini içerir. Eğitim setinin model oluşturmak amacıyla algoritma tarafından analiz edilmesiyle öğrenme basamağı gerçekleştirilir. Sınıflandırma aşaması oluşturulan modelin, karar ağacının doğruluğunu tespit etmek amacıyla test seti üzerinde test edilmesidir. Sınıflandırma işlemi karar ağacının kök düğümünde başlar ve sınıf etiketinin bulunduğu düğüme kadar özyinelemeli olarak ilerler. Her bir düğümde sağ veya sol alt ağaçtan hangisini seçerek ilerleyeceğine karar vermek için bölme koşulu uygulanır. Her durumda uygulanan bölme koşulu neticesinde olabildiğince homojen bir dağılım elde edilmelidir. Bunun içinde bölme kriteri denilen bir kavram ortaya çıkmıştır. Bölme kriteri matematiksel olarak hesaplanır ve en düşük değere sahip olan değer bölme koşulu olarak seçilir (Loh ve Shih, 1997). Şekil 3.14’te Karar ağacı algoritması kullanılarak yapılan sınıflandırma işlemi gösterilmiştir.



Şekil 3.14. Karar Ağacı algoritması kullanılarak yapılan sınıflandırma işlemi

Bölme kriterini hesaplamak için GINI indeksi, bilgi kazancı, kazanç oranı ve yanlış sınıflandırma oranı gibi birkaç hesaplama tekniği vardır. Bu çalışma kapsamında GINI indeksi ile devam edilecektir. Denklem 3.6, 3.7 ve 3.8’de GINI indeksi hesaplama formülleri

verilmiştir. GINI indeksi rastgele seçilen bir niteliğin olasılık değerini hesaplar. Bu olasılık değeri hesaplanmadan önce seçilen niteliğin sağ ve sol GINI değerleri hesaplandıktan sonra ortalama GINI değeri hesaplanır. Her bir nitelik için verilen formüllere göre hesaplanan GINI değerlerinden en küçük olanı baz alınarak sınıflandırma işlemi gerçekleştirilir. GINI indeksinin değeri 0 ile 1 arasında değişir. 0 olması yalnızca bir sınıf olduğunu ve tüm öğelerin o sınıfa dahil olduğunu gösterir, 1 olması tüm öğelerin çeşitli sınıflara rastgele dağıtıldığını gösterir, 0.5 olması ise bazı sınıflara eşit şekilde dağılımın gerçekleştiğini gösterir (Breiman ve ark., 1984)

$$\text{Gini}(L) = 1 - \sum_{i=1}^k \left[\frac{L_i}{|T_{sol}|} \right]^2 \quad (3.6)$$

$$\text{Gini}(R) = 1 - \sum_{i=1}^k \left[\frac{R_i}{|T_{sağ}|} \right]^2 \quad (3.7)$$

$$\text{Gini} = \frac{1}{n} (|T_{sol}| \text{Gini}_{sol} + |T_{sağ}| \text{Gini}_{sağ}) \quad (3.8)$$

K : Sınıfların sayısı

T : Bir düğümdeki örnek sayısı

T_{sol} : Sol koldaki örnek sayısı

T_{sağ} : Sağ koldaki örnek sayısı

R_i : Sağ koldaki i bölümündeki örnek sayısı

L_i : Sol koldaki i bölümündeki örnek sayısı

4. ARAŞTIRMA BULGULARI VE TARTIŞMA

Bu bölümde DDoS ataklarının tespitinde kullanılan yapay zeka temelli makine öğrenmesi algoritmaları olan K En Yakın Komşu, Rasgele Orman, Karar Ağacı ve Naive Bayes algoritmalarının CICDDoS2019 veri seti üzerinde uygulandığı deney ortamı, sonuçların değerlendirilmesi ve algoritmaların performansları karşılaştırılmıştır.

Algoritmaları test etmek için kullanılan bilgisayar Windows 11 OS, Intel(R) Core (TM) i7-10750H CPU 2.6 GHz işlemci, 16GB RAM, 1TB+256GB SSD ve GTX 1650 Ti Graphics Coprocessor özelliklerine sahiptir. Platform olarak Spyder 4.1.5 IDE, programlama dili olarak Python 3.8 ve Numpy, Seaborn, Pandas, Sklearn, Matplotlib kütüphaneleri kullanılmıştır.

4.1. Performans Metrikleri

K En Yakın Komşu, Rasgele Orman, Karar Ağacı ve Naive Bayes algoritmalarının ürettiği sonuçların değerlendirilmesinde Karmaşıklık Matrisi, Doğruluk, Duyarlılık, Kesinlik ve F1 Puanı ölçüm metrikleri kullanılmıştır.

-Karmaşıklık matrisi (Confusion Matrix): Karmaşıklık matrisi sınıflandırma problemlerinde tahmin sonuçlarının özetini sunan bir tablodur. Karmaşıklık matrisi metriğini kullanarak, sınıflandırmak için kullanılan algoritma yöntemi hakkında çıkarımlar yapılabilir. Literatürde çoğunlukla kullanılan performans ölçüm metriğidir. Çizelge 4.1’de karmaşıklık matrisi içeriği belirtilmiştir (Fawcett, 2006).

Çizelge 4.1. Karmaşıklık Matrisi

	Pozitif Tahmin	Negatif Tahmin
Gerçek Pozitif	Doğru Pozitif (TP)	Yanlış Negatif (FN)
Gerçek Negatif	Yanlış Pozitif (FP)	Doğru Negatif (TN)

Çizelgenin içeriğine bakılacak olursa karmaşıklık matrisi dört değer içermektedir. Bunlar;

- *Doğru Pozitif (TP):* Sınıflandırılacak verinin gerçek değerinin pozitif bir durumu ifade etmesi ve sınıflandırıcı tarafından pozitif olarak tahmin edilen örnekleri temsil eder.
- *Doğru Negatif (TN):* Sınıflandırılacak verinin gerçek değerinin negatif bir durumu ifade etmesi ve sınıflandırıcı tarafından negatif olarak tahmin edilen örnekleri temsil eder.

- *Yanlış Pozitif (FP)*: Sınıflandırılacak verinin gerçek değerinin negatif bir durumu ifade etmesi ve sınıflandırıcı tarafından pozitif olarak tahmin edilen örnekleri temsil eder.
- *Yanlış Negatif (FN)*: Sınıflandırılacak verinin gerçek değerinin pozitif bir durumu ifade etmesi ve sınıflandırıcı tarafından negatif olarak tahmin edilen örnekleri temsil eder.

-Doğruluk: 4.1 nolu eşitlikte gösterildiği üzere doğruluk, sınıflandırıcı tarafından doğru tahmin edilen örnek sayısının, tüm veri seti kümesinin sayısına bölünmesiyle hesaplanır. Bu değer ile sınıflandırıcının ne kadar doğru tahminde bulunduğu ölçülmektedir.

$$\text{Doğruluk (Accuracy)} = \frac{TP + TN}{TP + TN + FP + FN} \quad (4.1)$$

-Kesinlik: 4.2 nolu eşitlikte gösterildiği üzere kesinlik, sınıflandırıcı tarafından doğru pozitif olarak tahmin edilen örnek sayısının, pozitif olarak tahmin edilen örnek sayısına bölünmesiyle hesaplanır. Bu değer ile sınıflandırıcının yapmış olduğu pozitif tahminlerin ne kadarının doğru olduğu ölçülmektedir.

$$\text{Kesinlik (Precision)} = \frac{TP}{TP + FP} \quad (4.2)$$

-Duyarlılık: 4.3 nolu eşitlikte gösterildiği üzere, sınıflandırıcı tarafından doğru pozitif olarak tahmin edilen örnek sayısının, doğru pozitif ve yanlış negatif olarak tahmin edilen örnek sayısına bölünmesiyle hesaplanır. Sınıflandırıcının yapmış olduğu tüm pozitif tahminlerin kaç tanesinin gerçek pozitif olduğunu hesaplar.

$$\text{Duyarlılık (Sensitivity)} = \frac{TP}{TP + FN} \quad (4.3)$$

-F1 puanı: 4.4 nolu eşitlikte gösterildiği üzere F1 puanı, kesinlik ve geri çağırma arasındaki bağıntıyı gösterir. Bu değer kesinlik ve duyarlılık sonuçlarının harmonik ortalamasıdır. Daha çok dengesiz dağılım gösteren veri setlerinde kullanılmaktadır.

$$\text{F1 Puanı (F1 Score)} = 2 * \frac{\text{Kesinlik} * \text{Duyarlılık}}{\text{Kesinlik} + \text{Duyarlılık}} \quad (4.4)$$

4.2. Deneysel Sonuçlar

Dağıtık hizmet aksatma (DDoS) ataklarının tespit edilmesinde K En Yakın Komşu, Rastgele Orman, Karar Ağacı ve Naive Bayes algoritmalarının performansları incelenmiştir.

Algoritma performanslarını karşılaştırma amacıyla CICDDoS2019 veri seti kullanılmıştır. Veri seti Eğitim ve Test seti olmak üzere iki parçaya ayrılmıştır. Sonuçların genellenebilmesi için K-kat çapraz doğrulama kullanılmıştır. K-kat için “K” değeri hesaplama-zaman maliyeti ve literatürdeki çalışmalar göz önünde bulundurularak 5 olarak seçilmiştir (Kishore ve Devarakonda, 2021). Her bir algorithmadan elde edilen Eğitim ve Test sonuçları bu bölümde verilecektir.

4.2.1. K en yakın komşu algoritması kullanılarak elde edilen sonuçlar

KNN algoritması kullanılarak DDoS ataklarının tespit edilmesinde veri seti K-katlı çapraz doğrulama kullanılarak elde edilen sonuçlar çizelge olarak verilmiştir. Çizelgelerde verilen sonuçlar 5-kat çapraz doğrulama hesaplanmasının ortalama değerleridir. KNN algoritmasında “k” komşuluk değeri literatürde bulunan çalışmalara benzer şekilde 5 olarak seçilmiştir. KNN algoritmasında mesafe ölçüm metriği olarak Öklid mesafesi kullanılmıştır (Kishore ve Devarakonda, 2021).

Çizelge 4.2’de veri setinde bulunan tüm öznitelikler ve seçili öznitelikler kullanılarak gerçekleştirilen çoklu sınıflandırma işleminde elde edilen eğitim seti ve test seti için Doğruluk, Duyarlılık, Kesinlik ve F1 Puanı sonuçları ve tespit süreleri verilmiştir. Seçili öznitelikler kullanıldığında Doğruluk, Kesinlik, Duyarlılık, F1 Puanı düşmüş ancak tespit süresi azalmıştır.

Çizelge 4.2. KNN çoklu sınıflandırma sonuçları (5-Kat)

		Doğruluk	Kesinlik	Duyarlılık	F1 Puanı	Tespit Süresi
Eğitim Seti	Tüm öznitelikler	%99,99	%99,56	%99,34	%99,45	55,40 sn
	Seçilmiş öznitelikler	%93,98	%91,23	%89,45	%90,33	20,80 sn
Test Seti	Tüm öznitelikler	%99,98	%99,21	%98,09	%98,65	13,60 sn
	Seçilmiş öznitelikler	%92,99	%90,33	%89,19	%89,76	5,41 sn

Veri setinde bulunan tüm öznitelikler kullanılarak gerçekleştirilen çoklu sınıflandırma işleminde eğitim seti verileri için doğruluk oranı %99,99, kesinlik değeri %99,56, duyarlılık değeri %99,34, F1 puanı %99,45 olarak gerçekleşmiştir. Tespit süresi 55,40 saniye olarak gerçekleşmiştir. Test seti verileri için doğruluk oranı %99,98, kesinlik değeri %99,21, duyarlılık değeri %98,09, F1 puanı %98,65 olarak gerçekleşmiştir. Tespit süresi 13,60 saniye olarak gerçekleşmiştir.

Veri setinde bulunan seçilmiş öznitelikler kullanılarak gerçekleştirilen çoklu sınıflandırma işleminde eğitim seti verileri için doğruluk oranı %93,98, kesinlik değeri %91,23,

duyarlılık değeri %89,45, F1 puanı %90,33 olarak gerçekleşmiştir. Tespit süresi 20,80 saniye olarak gerçekleşmiştir. Test seti verileri için doğruluk oranı %92,99, kesinlik değeri %90,33, duyarlılık değeri %89,19, F1 puanı %89,76 olarak gerçekleşmiştir. Tespit süresi 5,41 saniye olarak gerçekleşmiştir.

Çizelge 4.3'te veri setinde bulunan tüm öznitelikler kullanılarak gerçekleştirilen ikili sınıflandırma işleminde elde edilen eğitim seti Doğruluk, Duyarlılık, Kesinlik ve F1 Puanı sonuçları ve tespit süreleri verilmiştir.

Çizelge 4.3. KNN tüm öznitelikler kullanılarak ikili sınıflandırma eğitim seti sonuçları (5-kat)

CCIDDOS2019 DDoS Atak Türü	Doğruluk	Kesinlik	Duyarlılık	F1 Puanı	Tespit Süresi
BENIGN	%99,99	%99,98	%99,99	%99,98	23,45 sn
LDAP	%99,98	%99,98	%99,96	%99,97	62,01 sn
UDP	%99,53	%99,51	%99,49	%99,50	65,20 sn
MSSQL	%99,95	%99,53	%99,34	%99,43	57,36 sn
NTP	%99,98	%99,89	%99,45	%99,67	60,48 sn
DNS	%99,93	%99,56	%99,51	%99,53	53,90 sn
SNMP	%99,97	%99,88	%99,83	%99,85	51,11 sn
NETBIOS	%99,99	%99,99	%99,99	%99,99	52,84 sn
TFTP	%99,12	%98,56	%98,34	%98,45	53,63 sn
PORTMAP	%99,34	%98,99	%97,56	%98,27	57,08 sn
WEBDDOS	%99,22	%99,45	%98,79	%99,12	61,57 sn
SYN	%99,33	%98,79	%98,02	%98,40	59,00 sn
UDP-LAG	%99,38	%99,09	%98,61	%98,85	55,06 sn

Veri setinde bulunan tüm öznitelikler kullanılarak gerçekleştirilen ikili sınıflandırma işleminde eğitim seti verileri için en yüksek doğruluk oranı atak olmayan paketlerin tespitinde ve NETBIOS ataklarının tespitinde %99,99 olarak gerçekleşmiştir. En düşük doğruluk oranı ise TFTP ataklarının tespit edilmesinde %99,12 olarak gerçekleşmiştir. En yüksek kesinlik değeri NETBIOS atakları tespitinde %99,99 olarak gerçekleşmiştir. En düşük kesinlik değeri TFTP atak tespitinde %98,56 olarak gerçekleşmiştir. En yüksek duyarlılık değeri atak olmayan paketlerin tespitinde ve NETBIOS atak tespitinde %99,99 olarak gerçekleşmiştir. En düşük duyarlılık değeri PORTMAP atak tespitinde %97,56 olarak gerçekleşmiştir. En yüksek F1 puanı NETBIOS atak tespitinde %99,99 olarak gerçekleşmiştir. En düşük F1 puanı PORTMAP atak tespitinde %98,27 olarak gerçekleşmiştir. En fazla süre 65,20 sn ile UDP atakları tespit edilirken, en az süre ise 23,45 sn ile atak olmayan paketler tespit edilirken harcanmıştır.

Çizelge 4.4'te veri setinde bulunan tüm öznitelikler kullanılarak gerçekleştirilen ikili sınıflandırma işleminde elde edilen test seti Doğruluk, Duyarlılık, Kesinlik ve F1 Puanı ölçüm ve tespit süreleri verilmiştir.

Çizelge 4.4. KNN tüm öznitelikler kullanılarak ikili sınıflandırma test seti sonuçları (5-kat)

CCIDDOS2019 DDoS Atak Türü	Doğruluk	Kesinlik	Duyarlılık	F1 Puanı	Tespit Süresi
BENIGN	%99,34	%98,56	%97,98	%98,27	5,86 sn
LDAP	%98,67	%98,45	%98,56	%98,50	15,50 sn
UDP	%96,79	%95,45	%91,31	%93,33	16,3 sn
MSSQL	%98,29	%95,44	%91,56	%93,46	14,34 sn
NTP	%96,45	%93,45	%95,79	%94,61	15,12 sn
DNS	%93,98	%91,23	%93,79	%92,49	13,47 sn
SNMP	%98,69	%98,07	%92,67	%95,29	12,77 sn
NETBIOS	%97,83	%94,56	%97,56	%96,04	13,21 sn
TFTP	%94,67	%92,45	%91,56	%92,00	13,40 sn
PORTMAP	%95,43	%94,56	%94,01	%94,28	14,27 sn
WEBDDOS	%98,92	%98,11	%97,45	%97,78	15,39 sn
SYN	%97,79	%95,33	%91,23	%93,23	14,75 sn
UDP-LAG	%98,45	%93,44	%95,45	%94,43	13,76 sn

Veri setinde bulunan tüm öznitelikler kullanılarak gerçekleştirilen ikili sınıflandırma işleminde test seti verileri için en yüksek doğruluk oranı atak olmayan paketlerin tespitinde %99,34 olarak gerçekleşmiştir. En düşük doğruluk oranı ise DNS ataklarının tespit edilmesinde %93,98 olarak gerçekleşmiştir. En yüksek kesinlik değeri atak olmayan paketlerin tespitinde %98,56 olarak gerçekleşmiştir. En düşük kesinlik değeri DNS atak tespitinde %91,23 olarak gerçekleşmiştir. En yüksek duyarlılık değeri LDAP atak tespitinde %98,56 olarak gerçekleşmiştir. En düşük duyarlılık değeri SYN atak tespitinde %91,23 olarak gerçekleşmiştir. En yüksek F1 puanı LDAP atak tespitinde %98,50 olarak gerçekleşmiştir. En düşük F1 puanı TFTP atak tespitinde %92,00 olarak gerçekleşmiştir. En fazla süre 16,3 sn ile UDP atakları tespit edilirken, en az süre ise 5,86 sn ile atak olmayan paketler tespit edilirken harcanmıştır.

Çizelge 4.5'te veri setinde bulunan seçilmiş öznitelikler kullanılarak gerçekleştirilen ikili sınıflandırma işleminde elde edilen eğitim seti Doğruluk, Duyarlılık, Kesinlik ve F1 Puanı sonuçları ve tespit süreleri verilmiştir.

Çizelge 4.5. KNN seçili öznitelikler kullanılarak ikili sınıflandırma eğitim sonuçları (5-kat)

CCIDDOS2019 DDoS Atak Türü	Doğruluk	Kesinlik	Duyarlılık	F1 Puanı	Tespit Süresi
BENIGN	%99,90	%99,55	%99,03	%99,29	26,54 sn
LDAP	%99,99	%99,55	%99,41	%99,48	27,11 sn
UDP	%99,39	%99,33	%99,23	%99,28	50,22 sn
MSSQL	%99,45	%98,97	%98,99	%98,98	41,29 sn
NTP	%99,56	%99,21	%99,07	%99,14	40,99 sn
DNS	%99,47	%98,48	%98,79	%98,63	47,05 sn
SNMP	%99,34	%98,08	%98,19	%98,13	44,21 sn
NETBIOS	%99,89	%99,25	%98,76	%99,00	25,74 sn
TFTP	%99,32	%98,49	%98,21	%98,35	27,73 sn
PORTMAP	%99,43	%98,19	%97,45	%97,82	21,18 sn
WEBDDOS	%99,34	%97,76	%98,91	%98,33	28,77 sn
SYN	%99,89	%98,50	%98,29	%98,39	47,89 sn
UDP-LAG	%99,21	%99,35	%98,67	%99,01	41,19 sn

Veri setinde bulunan seçili öznitelikler kullanılarak gerçekleştirilen ikili sınıflandırma işleminde eğitim seti verileri için en yüksek doğruluk oranı LDAP atak tespitinde %99,99 olarak gerçekleşmiştir. En düşük doğruluk oranı ise UDP-LAG ataklarının tespit edilmesinde %99,21 olarak gerçekleşmiştir. En yüksek kesinlik değeri atak olmayan paketlerin tespitinde ve LDAP atak tespitinde %99,55 olarak gerçekleşmiştir. En düşük kesinlik değeri WEBDDOS atak tespitinde %97,76 olarak gerçekleşmiştir. En yüksek duyarlılık değeri LDAP atak tespitinde %99,41 olarak gerçekleşmiştir. En düşük duyarlılık değeri PORTMAP atak tespitinde %97,45 olarak gerçekleşmiştir. En yüksek F1 puanı LDAP atak tespitinde %99,48 olarak gerçekleşmiştir. En düşük F1 puanı PORTMAP atak tespitinde %97,82 olarak gerçekleşmiştir. En fazla süre 50,22 sn ile UDP atakları tespit edilirken, en az süre ise 21,18 sn ile PORTMAP atakları tespit edilirken harcanmıştır.

Çizelge 4.6’te veri setinde bulunan seçilmiş öznitelikler kullanılarak gerçekleştirilen ikili sınıflandırma işleminde elde edilen test seti Doğruluk, Duyarlılık, Kesinlik ve F1 Puanı sonuçları ve tespit süreleri verilmiştir.

Çizelge 4.6. KNN seçili öznitelikler kullanılarak ikili sınıflandırma test seti sonuçları (5-kat)

CCIDDOS2019 DDoS Atak Türü	Doğruluk	Kesinlik	Duyarlılık	F1 Puanı	Tespit Süresi
BENIGN	%92,30	%89,67	%88,97	%89,32	3,63 sn
LDAP	%98,91	%91,45	%91,56	%91,50	6,77 sn
UDP	%96,78	%95,49	%97,31	%96,39	12,55 sn
MSSQL	%98,47	%95,41	%94,56	%94,98	10,32 sn
NTP	%96,21	%97,45	%95,79	%96,61	10,24 sn
DNS	%94,35	%93,23	%95,79	%94,49	11,76 sn
SNMP	%99,01	%91,07	%93,67	%92,35	11,05 sn
NETBIOS	%99,81	%95,56	%96,56	%96,06	6,43 sn
TFTP	%99,01	%99,45	%99,56	%99,50	6,93 sn
PORTMAP	%99,21	%94,56	%94,01	%94,28	5,29 sn
WEBDDOS	%99,11	%98,43	%97,69	%98,06	7,19 sn
SYN	%98,45	%99,01	%98,78	%98,89	11,97 sn
UDP-LAG	%98,39	%97,55	%97,78	%97,66	10,29 sn

Veri setinde bulunan seçili öznitelikler kullanılarak gerçekleştirilen ikili sınıflandırma işleminde test seti verileri için en yüksek doğruluk oranı %99,81 ile NETBIOS atak tespitinde, en düşük doğruluk oranı ise %92,30 ile atak olmayan paket tespitinde elde edilmiştir. En yüksek kesinlik değeri TFTP atak tespitinde %99,45 olarak gerçekleşmiştir. En düşük kesinlik değeri atak olmayan paketlerin tespitinde %89,67 olarak gerçekleşmiştir. En yüksek duyarlılık değeri TFTP atak tespitinde %99,56 olarak gerçekleşmiştir. En düşük duyarlılık değeri atak olmayan paketlerin tespitinde %88,97 olarak gerçekleşmiştir. En yüksek F1 puanı TFTP atak tespitinde %99,50 olarak gerçekleşmiştir. En düşük F1 puanı atak olmayan paketlerin tespitinde %89,32

olarak gerçekleşmiştir. En fazla süre 12,55 sn ile UDP atakları tespit edilirken, en az süre ise 3,63 sn ile atak olmayan paketler tespit edilirken harcanmıştır.

4.2.2. Naive Bayes (NB) algoritması kullanılarak elde edilen sonuçlar

NB algoritması kullanılarak DDoS ataklarının tespit edilmesinde veri seti K-katlı çapraz doğrulama kullanılarak elde edilen sonuçlar çizelge olarak verilmiştir. Çizelgelerde verilen sonuçlar 5-kat çapraz doğrulama hesaplanmasının ortalama değerleridir.

Çizelge 4.7’de veri setinde bulunan tüm öznitelikler ve seçili öznitelikler kullanılarak gerçekleştirilen çoklu sınıflandırma işleminde elde edilen eğitim seti ve test seti için Doğruluk, Duyarlılık, Kesinlik ve F1 Puanı sonuçları ve tespit süreleri verilmiştir. Seçili öznitelikler kullanıldığında Doğruluk, Kesinlik, Duyarlılık, F1 Puanı düşmüş ancak tespit süresi azalmıştır.

Çizelge 4.7. NB DDoS çoklu sınıflandırma sonuçları (5-Kat)

		Doğruluk	Kesinlik	Duyarlılık	F1 Puanı	Tespit Süresi
Eğitim Seti	Tüm öznitelikler	%87,45	%76,54	%84,67	%80,40	0,44 sn
	Seçilmiş öznitelikler	%83,44	%77,36	%80,78	%79,03	0,05 sn
Test Seti	Tüm öznitelikler	%86,34	%71,66	%82,36	%76,64	0,11 sn
	Seçilmiş öznitelikler	%82,49	%70,91	%79,45	%74,94	0,01 sn

Veri setinde bulunan tüm öznitelikler kullanılarak gerçekleştirilen çoklu sınıflandırma işleminde eğitim seti verileri için doğruluk oranı %87,45, kesinlik değeri %76,54, duyarlılık değeri %84,67, F1 puanı %80,40 olarak gerçekleşmiştir. Tespit süresi 0,44 saniye olarak gerçekleşmiştir. Test seti verileri için doğruluk oranı %86,34, kesinlik değeri %71,66, duyarlılık değeri %82,36, F1 puanı %76,64 olarak gerçekleşmiştir. Tespit süresi 0,11 saniye olarak gerçekleşmiştir.

Veri setinde bulunan seçilmiş öznitelikler kullanılarak gerçekleştirilen çoklu sınıflandırma işleminde eğitim seti verileri için doğruluk oranı %83,44, kesinlik değeri %77,36, duyarlılık değeri %80,78, F1 puanı %79,03 olarak gerçekleşmiştir. Tespit süresi 0,05 saniye olarak gerçekleşmiştir. Test seti verileri için doğruluk oranı %82,49 kesinlik değeri %70,91, duyarlılık değeri %79,45, F1 puanı %74,94 olarak gerçekleşmiştir. Tespit süresi 0,01 saniye olarak gerçekleşmiştir.

Çizelge 4.8’de veri setinde bulunan tüm öznitelikler kullanılarak gerçekleştirilen ikili sınıflandırma işleminde elde edilen eğitim seti Doğruluk, Duyarlılık, Kesinlik ve F1 Puanı sonuçları ve tespit süreleri verilmiştir.

Çizelge 4.8. NB tüm öznitelikler kullanılarak ikili sınıflandırma eğitim seti sonuçları (5-Kat)

CCIDDOS2019 DDoS Atak Türü	Doğruluk	Kesinlik	Duyarlılık	F1 Puanı	Tespit Süresi
BENIGN	%96,56	%95,16	%93,82	%94,49	0,08 sn
LDAP	%94,55	%94,47	%93,60	%94,03	0,12 sn
UDP	%87,90	%86,01	%96,34	%90,88	0,20 sn
MSSQL	%96,55	%95,98	%98,57	%97,26	0,20 sn
NTP	%72,35	%71,97	%85,17	%78,02	0,24 sn
DNS	%94,93	%93,08	%93,22	%93,15	0,24 sn
SNMP	%94,78	%93,75	%92,42	%93,08	0,24 sn
NETBIOS	%95,28	%94,35	%93,84	%94,09	0,24 sn
TFTP	%78,79	%78,77	%77,73	%78,25	0,12 sn
PORTMAP	%92,92	%92,99	%91,09	%92,03	0,24 sn
WEBDDOS	%94,08	%94,15	%93,54	%93,84	0,20 sn
SYN	%97,44	%96,14	%93,51	%94,81	0,16 sn
UDP-LAG	%96,76	%95,56	%95,87	%95,71	0,20 sn

Veri setinde bulunan tüm öznitelikler kullanılarak gerçekleştirilen ikili sınıflandırma işleminde eğitim seti verileri için en yüksek doğruluk SYN ataklarının tespitinde %97,44 olarak gerçekleşmiştir. En düşük doğruluk oranı ise NTP ataklarının tespit edilmesinde %72,35 olarak gerçekleşmiştir. En yüksek kesinlik değeri SYN atakları tespitinde %96,14 olarak gerçekleşmiştir. En düşük kesinlik değeri NTP atak tespitinde %71,97 olarak gerçekleşmiştir. En yüksek duyarlılık değeri MSSQL atak tespitinde %98,57 olarak gerçekleşmiştir. En düşük duyarlılık değeri TFTP atak tespitinde %77,73 olarak gerçekleşmiştir. En yüksek F1 puanı MSSQL atak tespitinde %97,26 olarak gerçekleşmiştir. En düşük F1 puanı NTP atak tespitinde %78,02 olarak gerçekleşmiştir. En fazla süre 0,24 sn ile NTP, DNS SNMP, NETBIOS ve PORTMAP atakları tespit edilirken, en az süre ise 0,08 sn ile atak olmayan paketler tespit edilirken harcanmıştır.

Çizelge 4.9’da veri setinde bulunan tüm öznitelikler kullanılarak gerçekleştirilen ikili sınıflandırma işleminde elde edilen test seti Doğruluk, Duyarlılık, Kesinlik ve F1 Puanı ve tespit süreleri verilmiştir.

Çizelge 4.9. NB tüm öznitelikler kullanılarak ikili sınıflandırma test seti sonuçları (5-Kat)

CCIDDOS2019 DDoS Atak Türü	Doğruluk	Kesinlik	Duyarlılık	F1 Puanı	Tespit Süresi
BENIGN	%95,56	%94,56	%92,78	%93,66	0,02 sn
LDAP	%93,43	%92,57	%91,60	%92,08	0,03 sn
UDP	%85,34	%85,85	%79,34	%82,47	0,05 sn
MSSQL	%95,03	%93,11	%92,47	%92,79	0,05 sn
NTP	%70,11	%70,11	%69,17	%69,64	0,06 sn
DNS	%93,07	%92,08	%89,22	%90,63	0,06 sn
SNMP	%93,45	%92,75	%89,12	%90,90	0,06 sn
NETBIOS	%92,34	%91,35	%91,04	%91,19	0,06 sn
TFTP	%77,56	%78,77	%76,82	%77,78	0,03 sn
PORTMAP	%91,85	%90,99	%90,45	%90,72	0,06 sn
WEBDDOS	%93,34	%91,15	%91,67	%91,41	0,05 sn
SYN	%96,12	%94,44	%95,81	%95,12	0,04 sn
UDP-LAG	%95,45	%91,56	%92,87	%92,21	0,05 sn

Veri setinde bulunan tüm öznitelikler kullanılarak gerçekleştirilen ikili sınıflandırma işleminde test seti verileri için en yüksek doğruluk oranı SYN atak tespitinde %96,12 olarak gerçekleşmiştir. En düşük doğruluk oranı ise NTP ataklarının tespit edilmesinde %70,11 olarak gerçekleşmiştir. En yüksek kesinlik değeri atak olmayan paketlerin tespitinde %94,56 olarak gerçekleşmiştir. En düşük kesinlik değeri NTP atak tespitinde %70,11 olarak gerçekleşmiştir. En yüksek duyarlılık değeri SYN atak tespitinde %95,81 olarak gerçekleşmiştir. En düşük duyarlılık değeri NTP atak tespitinde %69,17 olarak gerçekleşmiştir. En yüksek F1 puanı SYN atak tespitinde %95,12 olarak gerçekleşmiştir. En düşük F1 puanı NTP atak tespitinde %69,64 olarak gerçekleşmiştir. En fazla süre 0,06 sn ile NTP, DNS, SNMP, NETBIOS ve PORTMAP atakları tespit edilirken, en az süre ise 0,02 sn ile atak olmayan paketler tespit edilirken harcanmıştır.

Çizelge 4.10'da veri setinde bulunan seçilmiş öznitelikler kullanılarak gerçekleştirilen ikili sınıflandırma işleminde elde edilen eğitim seti Doğruluk, Duyarlılık, Kesinlik ve F1 Puanı sonuçları ve tespit süreleri verilmiştir.

Çizelge 4.10. NB seçilmiş öznitelikler kullanılarak ikili sınıflandırma eğitim seti sonuçları (5-Kat)

CCIDDOS2019 DDoS Atak Türü	Doğruluk	Kesinlik	Duyarlılık	F1 Puanı	Tespit Süresi
BENIGN	%97,08	%95,44	%94,32	%94,88	0,04 sn
LDAP	%99,57	%99,55	%99,11	%99,33	0,08 sn
UDP	%95,80	%95,80	%91,78	%93,75	0,04 sn
MSSQL	%98,02	%95,08	%96,08	%95,58	0,04 sn
NTP	%41,49	%41,46	%42,51	%41,98	0,04 sn
DNS	%99,95	%99,14	%98,30	%98,72	0,08 sn
SNMP	%99,78	%99,37	%98,74	%99,05	0,04 sn
NETBIOS	%97,28	%99,77	%99,70	%99,73	0,08 sn
TFTP	%88,98	%77,06	%76,39	%76,72	0,04 sn
PORTMAP	%99,84	%99,84	%99,68	%99,76	0,08 sn
WEBDDOS	%99,98	%99,98	%99,97	%99,97	0,04 sn
SYN	%99,78	%90,90	%94,75	%92,79	0,04 sn
UDP-LAG	%99,99	%99,98	%99,97	%99,97	0,04 sn

Veri setinde bulunan seçili öznitelikler kullanılarak gerçekleştirilen ikili sınıflandırma işleminde eğitim seti verileri için en yüksek doğruluk oranı UDP-LAG atak tespitinde %99,99 olarak gerçekleşmiştir. En düşük doğruluk oranı ise NTP ataklarının tespit edilmesinde %41,49 olarak gerçekleşmiştir. En yüksek kesinlik değeri WEBDDOS ve UDP-LAG atak tespitinde %99,98 olarak gerçekleşmiştir. En düşük kesinlik değeri NTP atak tespitinde %41,46 olarak gerçekleşmiştir. En yüksek duyarlılık değeri WEBDDOS ve UDP-LAG atak tespitinde %99,97 olarak gerçekleşmiştir. En düşük duyarlılık değeri NTP atak tespitinde %42,51 olarak gerçekleşmiştir. En yüksek F1 puanı WEBDDOS ve UDP-LAG atak tespitinde %99,97 olarak gerçekleşmiştir. En düşük F1 puanı NTP atak tespitinde %41,98 olarak gerçekleşmiştir. En

fazla süre 0,08 sn ile LDAP, DNS, NETBIOS, PORTMAP atakları tespit edilirken, en az süre ise 0,04 sn ile atak olmayan paketler, UDP, MSSQL, NTP, SNMP, TFTP, WEBDDOS, SYN, UDP-LAG atakları tespit edilirken harcanmıştır.

Çizelge 4.11’de veri setinde bulunan seçilmiş öznitelikler kullanılarak gerçekleştirilen ikili sınıflandırma işleminde elde edilen test seti Doğruluk, Duyarlılık, Kesinlik ve F1 Puanı sonuçları ve tespit süreleri verilmiştir.

Çizelge 4.11. NB seçilmiş öznitelikler kullanılarak ikili sınıflandırma test seti sonuçları (5-Kat)

CCIDDOS2019 DDoS Atak Türü	Doğruluk	Kesinlik	Duyarlılık	F1 Puanı	Tespit Süresi
BENIGN	%96,29	%93,42	%92,22	%92,82	0,01 sn
LDAP	%99,33	%97,54	%96,01	%96,77	0,02 sn
UDP	%90,34	%90,12	%89,69	%89,90	0,01 sn
MSSQL	%97,03	%92,87	%94,14	%93,50	0,01 sn
NTP	%41,23	%40,55	%40,05	%40,30	0,02 sn
DNS	%99,87	%96,18	%94,38	%95,27	0,02 sn
SNMP	%98,95	%97,67	%95,51	%96,58	0,01 sn
NETBIOS	%96,44	%95,87	%95,71	%95,79	0,02 sn
TFTP	%87,46	%74,16	%73,48	%73,82	0,01 sn
PORTMAP	%99,78	%98,81	%97,56	%98,18	0,02 sn
WEBDDOS	%99,87	%98,90	%98,29	%98,59	0,01 sn
SYN	%99,32	%88,98	%89,65	%89,31	0,01 sn
UDP-LAG	%99,55	%98,88	%98,45	%98,66	0,01 sn

Veri setinde bulunan seçili öznitelikler kullanılarak gerçekleştirilen ikili sınıflandırma işleminde test seti verileri için en yüksek doğruluk oranı %99,87 ile DNS, WEBDDOS atak tespitinde, en düşük doğruluk oranı ise %41,23 ile NTP atak tespitinde elde edilmiştir. En yüksek kesinlik değeri WEBDDOS tespitinde %98,90 olarak gerçekleşmiştir. En düşük kesinlik değeri NTP atak tespitinde %40,55 olarak gerçekleşmiştir. En yüksek duyarlılık değeri UDP-LAG atak tespitinde %98,45 olarak gerçekleşmiştir. En düşük duyarlılık değeri NTP atak tespitinde %40,05 olarak gerçekleşmiştir. En yüksek F1 puanı UDP-LAG atak tespitinde %98,66 olarak gerçekleşmiştir. En düşük F1 puanı NTP atak tespitinde %40,30 olarak gerçekleşmiştir. En fazla süre 0,02 sn ile LDAP, NTP, DNS, NETBIOS ve PORTMAP atakları tespit edilirken, en az süre ise 0,01 sn ile atak olmayan paketler, UDP, MSSQL, SNMP, TFTP, WEBDDOS, SYN, UDP-LAG atakları tespit edilirken harcanmıştır.

4.2.3. Rasgele Orman (RF) algoritması kullanılarak elde edilen sonuçlar

RF algoritması kullanılarak DDoS ataklarının tespit edilmesinde veri seti K-katlı çapraz doğrulama kullanılarak elde edilen sonuçlar çizelge olarak verilmiştir. Çizelgelerde verilen sonuçlar 5-kat çapraz doğrulama hesaplanmasının ortalama değerleridir.

RF algoritmasında maksimum derinlik değeri 1-17 arasındaki değerler için deneysel olarak belirlenmiştir. Sonuçlara göre en yüksek doğruluk değerine 9 değerinde ulaşıldığı için derinlik değeri 9 olarak seçilmiştir. Oluşturulacak ağaç sayısı da benzer şekilde 100-200 arasındaki değerler denenerek belirlenmiştir. En yüksek doğruluk oranına 104 değerinde ulaşılmıştır. Oluşturulacak ağaç sayısı 104 olarak seçilmiştir.

Çizelge 4.12’de veri setinde bulunan tüm öznitelikler ve seçili öznitelikler kullanılarak gerçekleştirilen çoklu sınıflandırma işleminde elde edilen eğitim seti ve test seti için Doğruluk, Duyarlılık, Kesinlik ve F1 Puanı sonuçları ve tespit süreleri verilmiştir. Seçili öznitelikler kullanıldığında Doğruluk, Kesinlik, Duyarlılık, F1 Puanı düşmüş ancak tespit süresi azalmıştır.

Çizelge 4.12. RF çoklu sınıflandırma sonuçları (5-Kat)

		Doğruluk	Kesinlik	Duyarlılık	F1 Puanı	Tespit Süresi
Eğitim Seti	Tüm öznitelikler	%99,99	%98,99	%98,95	%98,97	8,45 sn
	Seçilmiş öznitelikler	%97,56	%95,66	%96,77	%96,21	4,57 sn
Test Seti	Tüm öznitelikler	%99,78	%96,78	%95,98	%96,38	2,11 sn
	Seçilmiş öznitelikler	%94,56	%91,49	%94,56	%93,00	1,14 sn

Veri setinde bulunan tüm öznitelikler kullanılarak gerçekleştirilen çoklu sınıflandırma işleminde eğitim seti verileri için doğruluk oranı %99,99, kesinlik değeri %98,99, duyarlılık değeri %98,95, F1 puanı %98,97 olarak gerçekleşmiştir. Tespit süresi 8,45 saniye olarak gerçekleşmiştir. Test seti verileri için doğruluk oranı %99,78, kesinlik değeri %96,78, duyarlılık değeri %95,98, F1 puanı %96,38 olarak gerçekleşmiştir. Tespit süresi 2,11 saniye olarak gerçekleşmiştir.

Veri setinde bulunan seçilmiş öznitelikler kullanılarak gerçekleştirilen çoklu sınıflandırma işleminde eğitim seti verileri için doğruluk oranı %97,56, kesinlik değeri %95,66, duyarlılık değeri %96,77, F1 puanı %96,21 olarak gerçekleşmiştir. Tespit süresi 4,57 saniye olarak gerçekleşmiştir. Test seti verileri için doğruluk oranı %94,56, kesinlik değeri %91,49, duyarlılık değeri %94,56, F1 puanı %93,00 olarak gerçekleşmiştir. Tespit süresi 1,14 saniye olarak gerçekleşmiştir.

Çizelge 4.13’te veri setinde bulunan tüm öznitelikler kullanılarak gerçekleştirilen ikili sınıflandırma işleminde elde edilen eğitim seti Doğruluk, Duyarlılık, Kesinlik ve F1 Puanı sonuçları ve tespit süreleri verilmiştir.

Çizelge 4.13. RF tüm öznitelikler kullanılarak ikili sınıflandırma eğitim seti sonuçları (5-Kat)

CCIDDOS2019 DDoS Atak Türü	Doğruluk	Kesinlik	Duyarlılık	F1 Puanı	Tespit Süresi
BENIGN	%99,87	%99,45	%99,31	%99,38	2,4 sn
LDAP	%99,80	%99,23	%99,01	%99,12	2,4 sn
UDP	%99,42	%99,11	%98,79	%98,95	2,4 sn
MSSQL	%99,74	%98,67	%98,32	%98,49	2,4 sn
NTP	%99,96	%99,41	%99,56	%99,48	2,4 sn
DNS	%99,94	%99,57	%99,67	%99,62	2,0 sn
SNMP	%99,89	%99,45	%98,77	%99,11	2,4 sn
NETBIOS	%99,95	%99,67	%99,89	%99,78	2,5 sn
TFTP	%99,93	%99,78	%99,69	%99,73	1,7 sn
PORTMAP	%99,34	%99,21	%99,09	%99,15	1,6 sn
WEBDDOS	%99,91	%99,78	%99,69	%99,73	1,6 sn
SYN	%99,22	%98,81	%98,99	%98,90	2,0 sn
UDP-LAG	%99,99	%99,88	%99,85	%99,86	2,0 sn

Veri setinde bulunan tüm öznitelikler kullanılarak gerçekleştirilen ikili sınıflandırma işleminde eğitim seti verileri için en yüksek doğruluk oranı UDP-LAG ataklarının tespitinde %99,99 olarak gerçekleşmiştir. En düşük doğruluk oranı ise SYN ataklarının tespit edilmesinde %99,22 olarak gerçekleşmiştir. En yüksek kesinlik değeri UDP-LAG atakları tespitinde %99,88 olarak gerçekleşmiştir. En düşük kesinlik değeri MSSQL atak tespitinde %98,67 olarak gerçekleşmiştir. En yüksek duyarlılık değeri NETBIOS atak tespitinde %99,89 olarak gerçekleşmiştir. En düşük duyarlılık değeri MSSQL atak tespitinde %98,32 olarak gerçekleşmiştir. En yüksek F1 puanı UDP-LAG atak tespitinde %99,86 olarak gerçekleşmiştir. En düşük F1 puanı MSSQL atak tespitinde %98,49 olarak gerçekleşmiştir. En fazla süre 2,5 sn ile NETBIOS atakları tespit edilirken, en az süre ise 1,6 sn ile PORTMAP ve WEBDDOS atakları tespit edilirken harcanmıştır.

Çizelge 4.14'te veri setinde bulunan tüm öznitelikler kullanılarak gerçekleştirilen ikili sınıflandırma işleminde elde edilen test seti Doğruluk, Duyarlılık, Kesinlik ve F1 Puanı ölçüm ve tespit süreleri verilmiştir.

Çizelge 4.14. RF tüm öznitelikler kullanılarak ikili sınıflandırma test seti sonuçları (5-Kat)

CCIDDOS2019 DDoS Atak Türü	Doğruluk	Kesinlik	Duyarlılık	F1 Puanı	Tespit Süresi
BENIGN	%98,56	%97,89	%97,99	%97,94	0,6 sn
LDAP	%99,45	%99,07	%98,39	%98,73	0,6 sn
UDP	%99,12	%98,42	%98,46	%98,44	0,6 sn
MSSQL	%99,70	%98,73	%98,75	%98,74	0,6 sn
NTP	%99,57	%99,34	%98,53	%98,93	0,6 sn
DNS	%99,67	%98,90	%98,21	%98,55	0,5 sn
SNMP	%99,13	%97,87	%97,03	%97,45	0,6 sn
NETBIOS	%99,91	%98,56	%97,78	%98,17	0,6 sn
TFTP	%99,32	%97,31	%98,29	%97,80	0,4 sn
PORTMAP	%98,79	%97,27	%96,34	%96,80	0,4 sn
WEBDDOS	%97,99	%97,41	%96,56	%96,98	0,4 sn
SYN	%99,04	%98,02	%97,78	%97,90	0,5 sn
UDP-LAG	%99,78	%99,65	%99,31	%99,48	0,5 sn

Veri setinde bulunan tüm öznitelikler kullanılarak gerçekleştirilen ikili sınıflandırma işleminde test seti verileri için en yüksek başarı oranı %99,91 ile NETBIOS ataklarının tespitinde, en düşük başarı oranı ise %97,99 ile WEBDDOS ataklarının tespitinde elde edilmiştir. En yüksek kesinlik değeri UDP-LAG atak tespitinde %99,65 olarak gerçekleşmiştir. En düşük kesinlik değeri PORTMAP atak tespitinde %97,27 olarak gerçekleşmiştir. En yüksek duyarlılık değeri UDP-LAG atak tespitinde %99,31 olarak gerçekleşmiştir. En düşük duyarlılık değeri PORTMAP atak tespitinde %96,34 olarak gerçekleşmiştir. En yüksek F1 puanı UDP-LAG atak tespitinde %99,48 olarak gerçekleşmiştir. En düşük F1 puanı PORTMAP atak tespitinde %96,80 olarak gerçekleşmiştir. En fazla süre 0,6 sn ile atak olmayan paketler, LDAP, UDP, MSSQL, NTP, SNMP, NETBIOS atakları tespit edilirken, en az süre ise 0,4 sn ile TFTP, PORTMAP, WEBDDOS atakları tespit edilirken harcanmıştır.

Çizelge 4.15'te veri setinde bulunan seçilmiş öznitelikler kullanılarak gerçekleştirilen ikili sınıflandırma işleminde elde edilen eğitim seti Doğruluk, Duyarlılık, Kesinlik ve F1 Puanı sonuçları ve tespit süreleri verilmiştir.

Çizelge 4.15. RF seçili öznitelikler kullanılarak ikili sınıflandırma eğitim seti sonuçları (5-Kat)

CCIDDOS2019 DDoS Atak Türü	Doğruluk	Kesinlik	Duyarlılık	F1 Puanı	Tespit Süresi
BENIGN	%95,46	%94,56	%93,67	%94,11	0,9 sn
LDAP	%99,56	%99,09	%99,21	%99,15	1,6 sn
UDP	%97,00	%96,04	%94,00	%95,01	1,2 sn
MSSQL	%98,39	%96,42	%98,34	%97,37	1,2 sn
NTP	%99,87	%99,69	%98,45	%99,07	1,2 sn
DNS	%99,28	%98,99	%98,43	%98,71	2,0 sn
SNMP	%99,63	%99,01	%99,21	%99,11	1,6 sn
NETBIOS	%99,85	%99,45	%99,41	%99,43	1,2 sn
TFTP	%99,92	%99,42	%98,41	%98,91	2,0 sn
PORTMAP	%99,84	%98,79	%98,45	%98,62	1,6 sn
WEBDDOS	%99,88	%99,01	%98,88	%98,94	1,6 sn
SYN	%99,80	%99,45	%99,07	%99,26	1,6 sn
UDP-LAG	%99,98	%99,56	%98,70	%99,13	1,3 sn

Veri setinde bulunan seçili öznitelikler kullanılarak gerçekleştirilen ikili sınıflandırma işleminde eğitim seti verileri için en yüksek doğruluk oranı UDP-LAG ataklarının tespitinde %99,98 olarak gerçekleşmiştir. En düşük doğruluk oranı ise atak olmayan paketlerin tespit edilmesinde %95,46 olarak gerçekleşmiştir. En yüksek kesinlik değeri NTP atak tespitinde %99,69 olarak gerçekleşmiştir. En düşük kesinlik değeri atak olmayan paketlerin tespitinde %94,56 olarak gerçekleşmiştir. En yüksek duyarlılık değeri NETBIOS atak tespitinde %99,41 olarak gerçekleşmiştir. En düşük duyarlılık değeri atak olmayan paketlerin tespitinde %93,67 olarak gerçekleşmiştir. En yüksek F1 puanı NETBIOS atak tespitinde %99,43 olarak gerçekleşmiştir. En düşük F1 puanı atak olmayan paketlerin tespitinde %94,11 olarak

gerçekleşmiştir. En fazla süre 2,00 sn ile DNS ve TFTP atakları tespit edilirken, en az süre ise 0,9 sn ile atak olmayan paketler tespit edilirken harcanmıştır.

Çizelge 4.16’da veri setinde bulunan seçilmiş öznitelikler kullanılarak gerçekleştirilen ikili sınıflandırma işleminde elde edilen test seti Doğruluk, Duyarlılık, Kesinlik ve F1 Puanı sonuçları ve tespit süreleri verilmiştir.

Çizelge 4.16. RF seçili öznitelikler kullanılarak ikili sınıflandırma test seti sonuçları (5-Kat)

CCIDDOS2019 DDoS Atak Türü	Doğruluk	Kesinlik	Duyarlılık	F1 Puanı	Tespit Süresi
BENIGN	%94,56	%93,44	%92,99	%93,21	0,2 sn
LDAP	%99,34	%98,78	%98,43	%98,60	0,4 sn
UDP	%96,45	%95,67	%93,50	%94,57	0,3 sn
MSSQL	%97,89	%95,43	%95,19	%95,31	0,3 sn
NTP	%99,67	%98,89	%97,43	%98,15	0,3 sn
DNS	%99,01	%97,99	%98,09	%98,04	0,5 sn
SNMP	%99,43	%98,45	%98,10	%98,27	0,4 sn
NETBIOS	%99,12	%98,78	%98,43	%98,60	0,3 sn
TFTP	%99,23	%98,99	%98,68	%98,83	0,5 sn
PORTMAP	%99,11	%97,99	%98,04	%98,01	0,4 sn
WEBDDOS	%99,03	%98,87	%97,86	%98,36	0,4 sn
SYN	%99,31	%98,79	%98,45	%98,62	0,4 sn
UDP-LAG	%99,61	%98,45	%97,89	%98,17	0,3 sn

Veri setinde bulunan seçili öznitelikler kullanılarak gerçekleştirilen ikili sınıflandırma işleminde test seti verileri için en yüksek başarı oranı %99,67 ile NTP atak tespitinde, en düşük başarı oranı ise %94,56 ile atak olmayan paket tespitinde elde edilmiştir. En yüksek kesinlik değeri TFTP tespitinde %98,99 olarak gerçekleşmiştir. En düşük kesinlik değeri atak olmayan paketlerin tespitinde %93,44 olarak gerçekleşmiştir. En yüksek duyarlılık değeri TFTP atak tespitinde %98,68 olarak gerçekleşmiştir. En düşük duyarlılık değeri atak olmayan paketlerin tespitinde %92,99 olarak gerçekleşmiştir. En yüksek F1 puanı TFTP atak tespitinde %98,83 olarak gerçekleşmiştir. En düşük F1 puanı atak olmayan paketlerin tespitinde %93,21 olarak gerçekleşmiştir. En fazla süre 0,5 sn ile DNS ve TFTP atakları tespit edilirken, en az süre ise 0,2 sn ile atak olmayan paketler tespit edilirken harcanmıştır.

4.2.4. Karar ağacı (DT) algoritması kullanılarak elde edilen sonuçlar

DT algoritması kullanılarak DDoS ataklarının tespit edilmesinde veri seti K-katlı çapraz doğrulama kullanılarak elde edilen sonuçlar çizelge olarak verilmiştir. Çizelgelerde verilen sonuçlar 5-kat çapraz doğrulama hesaplanmasının ortalama değerleridir. DT algoritmasında maksimum derinlik değeri 1-17 arasındaki değerler deneysel olarak belirlenmiştir. Sonuçlara göre en yüksek doğruluk değerine 9 değerinde ulaşıldığı için derinlik değeri 9 olarak seçilmiştir.

Çizelge 4.17’de veri setinde bulunan tüm öznitelikler ve seçili öznitelikler kullanılarak gerçekleştirilen çoklu sınıflandırma işleminde elde edilen eğitim seti ve test seti için Doğruluk, Duyarlılık, Kesinlik ve F1 Puanı sonuçları ve tespit süreleri verilmiştir. Seçili öznitelikler kullanıldığında Doğruluk, Kesinlik, Duyarlılık, F1 Puanı düşmüş ancak tespit süresi azalmıştır.

Çizelge 4.17. DT çoklu sınıflandırma sonuçları (5-Kat)

		Doğruluk	Kesinlik	Duyarlılık	F1 Puanı	Tespit Süresi
Eğitim Seti	Tüm öznitelikler	%99,99	%98,99	%98,77	%98,88	0,13 sn
	Seçilmiş öznitelikler	%94,98	%88,76	%89,99	%89,37	0,03 sn
Test Seti	Tüm öznitelikler	%99,98	%96,45	%94,45	%95,44	0,03 sn
	Seçilmiş öznitelikler	%93,99	%81,66	%83,67	%82,65	0,01 sn

Veri setinde bulunan tüm öznitelikler kullanılarak gerçekleştirilen çoklu sınıflandırma işleminde eğitim seti verileri için doğruluk oranı %99,99, kesinlik değeri %98,99, duyarlılık değeri %98,77, F1 puanı %98,88 olarak gerçekleşmiştir. Tespit süresi 0,13 saniye olarak gerçekleşmiştir. Test seti verileri için doğruluk oranı %99,98, kesinlik değeri %96,45, duyarlılık değeri %94,45, F1 puanı %95,44 olarak gerçekleşmiştir. Tespit süresi 0,03 saniye olarak gerçekleşmiştir.

Veri setinde bulunan seçilmiş öznitelikler kullanılarak gerçekleştirilen çoklu sınıflandırma işleminde eğitim seti verileri için doğruluk oranı %94,98, kesinlik değeri %88,76, duyarlılık değeri %89,99, F1 puanı %89,37 olarak gerçekleşmiştir. Tespit süresi 0,03 saniye olarak gerçekleşmiştir. Test seti verileri için doğruluk oranı %93,99, kesinlik değeri %81,66, duyarlılık değeri %83,67, F1 puanı %82,65 olarak gerçekleşmiştir. Tespit süresi 0,01 saniye olarak gerçekleşmiştir.

Çizelge 4.18’de veri setinde bulunan tüm öznitelikler kullanılarak gerçekleştirilen ikili sınıflandırma işleminde elde edilen eğitim seti Doğruluk, Duyarlılık, Kesinlik ve F1 Puanı sonuçları verilmiştir.

Çizelge 4.18. DT tüm öznitelikler kullanılarak ikili sınıflandırma eğitim seti sonuçları (5-Kat)

CCIDDOS2019 DDoS Atak Türü	Doğruluk	Kesinlik	Duyarlılık	F1 Puanı	Tespit Süresi
BENIGN	%99,56	%98,18	%98,04	%98,11	0,05 sn
LDAP	%99,99	%99,99	%99,99	%99,99	0,11 sn
UDP	%99,50	%99,49	%99,52	%99,50	0,05 sn
MSSQL	%99,97	%99,97	%99,87	%99,92	0,05 sn
NTP	%100	%99,99	%99,79	%99,89	0,05 sn
DNS	%99,59	%99,95	%99,87	%99,91	0,05 sn
SNMP	%99,96	%99,99	%99,54	%99,76	0,05 sn
NETBIOS	%99,98	%99,54	%99,02	%99,28	0,05 sn
TFTP	%99,95	%99,21	%98,78	%98,99	0,08 sn
PORTMAP	%99,79	%99,34	%99,56	%99,45	0,04 sn
WEBDDOS	%100	%99,99	%99,98	%99,98	0,08 sn
SYN	%99,98	%99,97	%99,29	%99,63	0,06 sn
UDP-LAG	%99,99	%99,87	%99,45	%99,66	0,04 sn

Veri setinde bulunan tüm öznitelikler kullanılarak gerçekleştirilen ikili sınıflandırma işleminde eğitim seti verileri için en yüksek doğruluk oranı NTP ve WEBDDOS ataklarının tespitinde %100 olarak gerçekleşmiştir. En düşük doğruluk oranı ise UDP ataklarının tespit edilmesinde %99,50 olarak gerçekleşmiştir. En yüksek kesinlik değeri LDAP, NTP, SNMP ve WEBDDOS atakları tespitinde %99,99 olarak gerçekleşmiştir. En düşük kesinlik değeri atak olmayan paketlerin tespitinde %98,18 olarak gerçekleşmiştir. En yüksek duyarlılık değeri LDAP atak tespitinde %99,99 olarak gerçekleşmiştir. En düşük duyarlılık değeri atak olmayan paketlerin tespitinde %98,04 olarak gerçekleşmiştir. En yüksek F1 puanı LDAP atak tespitinde %99,99 olarak gerçekleşmiştir. En düşük F1 puanı atak olmayan paketlerin tespitinde %98,11 olarak gerçekleşmiştir. En fazla süre 0,11 sn ile LDAP atakları tespit edilirken, en az süre ise 0,04 sn ile PORTMAP ve UDP-LAG atakları tespit edilirken harcanmıştır.

Çizelge 4.19’da veri setinde bulunan tüm öznitelikler kullanılarak gerçekleştirilen ikili sınıflandırma işleminde elde edilen test seti Doğruluk, Duyarlılık, Kesinlik ve F1 Puanı ölçüm ve tespit süreleri verilmiştir.

Çizelge 4.19. DT tüm öznitelikler kullanılarak ikili sınıflandırma test seti sonuçları (5-Kat)

CCIDDOS2019 DDoS Atak Türü	Doğruluk	Kesinlik	Duyarlılık	F1 Puanı	Tespit Süresi
BENIGN	%98,79	%97,78	%97,21	%97,49	0,01 sn
LDAP	%99,78	%99,34	%99,45	%99,39	0,02 sn
UDP	%99,02	%98,35	%98,55	%98,45	0,01 sn
MSSQL	%99,78	%99,01	%98,78	%98,89	0,01 sn
NTP	%99,97	%99,67	%99,55	%99,61	0,01 sn
DNS	%99,29	%98,56	%98,45	%98,50	0,01 sn
SNMP	%99,67	%98,99	%99,15	%99,07	0,01 sn
NETBIOS	%99,78	%99,21	%98,88	%99,04	0,01 sn
TFTP	%99,34	%98,79	%98,41	%98,60	0,02 sn
PORTMAP	%99,23	%98,21	%97,55	%97,88	0,01 sn
WEBDDOS	%99,99	%99,54	%99,67	%99,60	0,02 sn
SYN	%99,34	%98,99	%98,71	%98,85	0,01 sn
UDP-LAG	%99,65	%98,91	%97,56	%98,23	0,01 sn

Veri setinde bulunan tüm öznitelikler kullanılarak gerçekleştirilen ikili sınıflandırma işleminde test seti verileri için en yüksek doğruluk oranı %99,99 ile WEBDDOS ataklarının tespitinde, en düşük doğruluk oranı ise %98,79 ile atak olmayan paketlerin tespitinde elde edilmiştir. En yüksek kesinlik değeri NTP atak tespitinde %99,67 olarak gerçekleşmiştir. En düşük kesinlik değeri atak olmayan paketlerin tespitinde %97,78 olarak gerçekleşmiştir. En yüksek duyarlılık değeri WEBDDOS atak tespitinde %99,67 olarak gerçekleşmiştir. En düşük duyarlılık değeri atak olmayan paketlerin tespitinde %97,21 olarak gerçekleşmiştir. En yüksek F1 puanı NTP atak tespitinde %99,61 olarak gerçekleşmiştir. En düşük F1 puanı atak olmayan paketlerin tespitinde %97,49 olarak gerçekleşmiştir. En fazla süre 0,02 saniye ile LDAP, TFTP, WEBDDOS atakları tespit edilirken, en az süre ise 0,01 saniye ile atak olmayan paketler, UDP,

MSSQL, NTP, DNS, SNMP, NETBIOS, PORTMAP, SYN, UDP-LAG atakları tespit edilirken harcanmıştır.

Çizelge 4.20’de veri setinde bulunan seçilmiş öznitelikler kullanılarak gerçekleştirilen ikili sınıflandırma işleminde elde edilen eğitim seti Doğruluk, Duyarlılık, Kesinlik ve F1 Puanı sonuçları verilmiştir.

Çizelge 4.20. DT seçilmiş öznitelikler kullanılarak ikili sınıflandırma eğitim seti sonuçları (5-Kat)

CCIDDOS2019 DDoS Atak Türü	Doğruluk	Kesinlik	Duyarlılık	F1 Puanı	Tespit Süresi
BENIGN	%95,67	%93,44	%93,78	%93,61	0,012 sn
LDAP	%99,56	%99,33	%99,39	%99,36	0,015 sn
UDP	%97,05	%97,01	%98,01	%97,51	0,025 sn
MSSQL	%98,25	%98,33	%98,38	%98,35	0,031 sn
NTP	%99,87	%99,87	%99,88	%99,87	0,032 sn
DNS	%99,26	%99,26	%99,05	%99,15	0,032 sn
SNMP	%99,61	%99,59	%99,59	%99,59	0,020 sn
NETBIOS	%99,85	%99,84	%99,73	%99,78	0,020 sn
TFTP	%99,92	%99,91	%98,26	%99,08	0,028 sn
PORTMAP	%99,84	%99,84	%99,81	%99,82	0,025 sn
WEBDDOS	%99,98	%99,98	%99,98	%99,98	0,013 sn
SYN	%99,82	%99,81	%99,82	%99,81	0,032 sn
UDP-LAG	%99,98	%99,81	%99,49	%99,65	0,024 sn

Veri setinde bulunan seçili öznitelikler kullanılarak gerçekleştirilen ikili sınıflandırma işleminde eğitim seti verileri için en yüksek doğruluk oranı WEBDDOS ve UDP-LAG ataklarının tespitinde %99,98 olarak gerçekleşmiştir. En düşük doğruluk oranı ise atak olmayan paketlerin tespit edilmesinde %95,67 olarak gerçekleşmiştir. En yüksek kesinlik değeri WEBDDOS atak tespitinde %99,98 olarak gerçekleşmiştir. En düşük kesinlik değeri atak olmayan paketlerin tespitinde %93,44 olarak gerçekleşmiştir. En yüksek duyarlılık değeri WEBDDOS atak tespitinde %99,98 olarak gerçekleşmiştir. En düşük duyarlılık değeri atak olmayan paketlerin tespitinde %93,78 olarak gerçekleşmiştir. En yüksek F1 puanı WEBDDOS atak tespitinde %99,98 olarak gerçekleşmiştir. En düşük F1 puanı atak olmayan paketlerin tespitinde %93,61 olarak gerçekleşmiştir. En fazla süre 0,032 saniye ile NTP, DNS ve SYN atakları tespit edilirken, en az süre ise 0,12 saniye ile atak olmayan paketler tespit edilirken harcanmıştır.

Çizelge 4.21’de veri setinde bulunan seçilmiş öznitelikler kullanılarak gerçekleştirilen ikili sınıflandırma işleminde elde edilen test seti Doğruluk, Duyarlılık, Kesinlik ve F1 Puanı sonuçları verilmiştir.

Çizelge 4.21. DT seçilmiş öznitelikler kullanılarak ikili sınıflandırma test seti sonuçları (5-Kat)

CCIDDOS2019 DDoS Atak Türü	Doğruluk	Kesinlik	Duyarlılık	F1 Puanı	Tespit Süresi
BENIGN	%93,56	%92,34	%92,76	%92,55	0,003 sn
LDAP	%99,45	%98,71	%98,11	%98,41	0,005 sn
UDP	%96,45	%95,21	%96,34	%95,77	0,006 sn
MSSQL	%97,32	%96,23	%95,54	%95,88	0,008 sn
NTP	%98,78	%97,41	%97,33	%97,37	0,008 sn
DNS	%98,01	%97,43	%97,99	%97,71	0,009 sn
SNMP	%98,23	%98,01	%98,18	%98,09	0,007 sn
NETBIOS	%98,84	%98,45	%98,21	%98,33	0,005 sn
TFTP	%98,24	%97,50	%97,98	%97,74	0,007 sn
PORTMAP	%98,45	%98,49	%98,19	%98,34	0,006 sn
WEBDDOS	%98,48	%98,65	%98,34	%98,49	0,003 sn
SYN	%98,34	%98,15	%98,21	%98,18	0,008 sn
UDP-LAG	%98,56	%97,65	%97,99	%97,82	0,006 sn

Veri setinde bulunan seçili öznitelikler kullanılarak gerçekleştirilen ikili sınıflandırma işleminde test seti verileri için en yüksek doğruluk oranı %99,45 ile LDAP ataklarının tespitinde, en düşük doğruluk oranı %93,56 ile atak olmayan paket tespitinde elde edilmiştir. En yüksek kesinlik değeri LDAP atak tespitinde %98,71 olarak gerçekleşmiştir. En düşük kesinlik değeri atak olmayan paketlerin tespitinde %92,34 olarak gerçekleşmiştir. En yüksek duyarlılık değeri WEBDDOS atak tespitinde %98,34 olarak gerçekleşmiştir. En düşük duyarlılık değeri atak olmayan paketlerin tespitinde %92,76 olarak gerçekleşmiştir. En yüksek F1 puanı WEBDDOS atak tespitinde %98,49 olarak gerçekleşmiştir. En düşük F1 puanı atak olmayan paketlerin tespitinde %92,55 olarak gerçekleşmiştir. En fazla süre 0,009 saniye ile DNS atakları tespit edilirken, en az süre ise 0,003 saniye ile atak olmayan paketler ve WEBDDOS atakları tespit edilirken harcanmıştır.

4.2.5. Algoritmaların performanslarının karşılaştırılması

Gerçek hayat uygulamalarında genel olarak atak içeren paketlerin atak türüne bakılmaksızın engellenmesi, atak olmayan paketlerin ise ağ trafiğine dahil edilmesi yaklaşımı tercih edilir. Çizelge 4.22’de test verileri için tüm öznitelikler kullanılarak yapılan ikili sınıflandırma işleminde atak olmayan paketlerin tespitinde çalışma kapsamında ele alınan algoritmaların sonuçları verilmiştir.

Çizelge 4.22. Test setinde yer alan tüm öz nitelikler kullanıldığında algoritmaların atak olmayan paketleri tespit sonuçları (5-Kat)

Model	Doğruluk	Kesinlik	Duyarlılık	F1 Puanı	Tespit Süresi
KNN	%99,34	%98,56	%97,98	%98,27	5,86 sn
NB	%95,56	%94,56	%92,78	%93,66	0,02 sn
RF	%98,56	%97,89	%97,99	%97,94	0,6 sn
DT	%98,79	%97,78	%97,21	%97,49	0,01 sn

En yüksek doğruluk oranı %99,34 ile KNN algoritmasında, en düşük doğruluk oranı %95,56 ile NB algoritmasında elde edilmiştir. En yüksek kesinlik değeri %98,56 ile KNN algoritmasında, en düşük kesinlik değeri %94,56 ile NB algoritmasında elde edilmiştir. En yüksek duyarlılık değeri %97,99 ile RF algoritmasında, en düşük duyarlılık değeri %92,78 ile NB algoritmasında elde edilmiştir. En yüksek F1 puanı %98,27 ile KNN algoritmasında, en düşük F1 puanı %93,66 ile NB algoritmasında elde edilmiştir. En fazla süre 5,86 saniye ile KNN algoritmasının sonuç üretmesinde, en az süre ise 0,01 saniye ile DT algoritmasının sonuç üretmesinde harcanmıştır.

Çizelge 4.23'te test verileri için seçili öz nitelikler kullanılarak yapılan ikili sınıflandırma işleminde atak olmayan paketlerin tespitinde çalışma kapsamında ele alınan algoritmaların sonuçları verilmiştir.

Çizelge 4.23. Test setinde yer alan seçili öz nitelikler kullanıldığında algoritmaların atak olmayan paketleri tespit sonuçları (5-Kat)

Model	Doğruluk	Kesinlik	Duyarlılık	F1 Puanı	Tespit Süresi
KNN	%92,30	%89,67	%88,97	%89,32	3,63 sn
NB	%96,29	%93,42	%92,22	%92,82	0.01 sn
RF	%94,56	%93,44	%92,99	%93,21	0,2 sn
DT	%93,56	%92,34	%92,76	%92,55	0.003 sn

En yüksek doğruluk oranı %96,29 ile NB algoritmasında, en düşük doğruluk oranı %92,30 ile KNN algoritmasında elde edilmiştir. En yüksek kesinlik değeri %93,44 ile RF algoritmasında, en düşük kesinlik değeri %89,67 ile KNN algoritmasında elde edilmiştir. En yüksek duyarlılık değeri %92,99 ile RF algoritmasında, en düşük duyarlılık değeri %88,97 ile KNN algoritmasında elde edilmiştir. En yüksek F1 puanı %93,21 ile RF algoritmasında, en düşük F1 puanı %89,32 ile KNN algoritmasında elde edilmiştir. En fazla süre 3,63 saniye ile KNN algoritmasının sonuç üretmesinde, en az süre ise 0,003 saniye ile DT algoritmasının sonuç üretmesinde harcanmıştır.

Bu çalışma çerçevesinde CCIDDOS2019 veri seti kullanılmıştır. Literatürde CCIDDOS2019 veri seti kullanılarak yapılan çalışmaların sonuçları ile bu çalışmanın sonuçlarının karşılaştırılması Çizelge 4.24'te verilmiştir.

Çizelge 4.24. CCIDDOS2019 veri seti kullanılarak gerçekleştirilen çalışmaların karşılaştırılması					
	Çalışma	En başarılı algoritma	Veri seti bölünme oranı	Doğruluk	Tespit süresi
Çoklu Sınıflandırma	(Sharafaldine ve ark, 2019)	ID3	K-Kat (k=5)	%78	4,53 sn
	(Alzahrani ve ark, 2021)	DT	-	%99,87	-
	(Batchu ve Seetha, 2021)	Gradyan Artırma	-	%99,97	-
	(Thorat ve ark., 2021)	TaxoDaCML	(%20-%80)	%99,9	-
	(Santhosh ve ark, 2023)	Modifiye edilmiş XGBOOST	-	%97	-
	Gerçekleştirilen çalışma	RF	K-Kat (k=5)	%94,56	1,14 sn
İkili Sınıflandırma	(Elsayed ve ark, 2020)	DDoSNet	(%30-%70)	%99	-
	(Çil ve ark, 2021)	DNN	(%20-%80)	%94,57	-
	(Kishore ve Devarakonda, 2021)	DT	K-Kat (k=5)	%99,88	-
	(Mistry, 2023)	DT	(%20-%80)	%97,70	3,02 sn
	Gerçekleştirilen çalışma	NB	K-Kat (k=5)	%96,29	0,01 sn

Çalışma kapsamında kullanılan algoritmaların çoklu sınıflandırma test seti sonuçları ele alındığında; K-Kat değerinin 5 olduğu çalışmalara göre en yüksek doğruluk oranı RF algoritması kullanılarak %94,56 olarak belirlenmiştir. Tespit süreleri açısından değerlendirildiğinde RF algoritmasının atakları tespit süresi 1,14 sn olarak belirlenmiştir.

İkili sınıflandırma test seti sonuçları ele alındığında; K-Kat değerinin 5 olduğu çalışmalara göre en yüksek doğruluk oranı DT algoritması ile %99,88 olduğu gözlenmiştir (Kishore ve Devarakonda, 2021). Gerçekleştirilen çalışmada ise ikili sınıflandırmada en yüksek doğruluk oranı NB algoritması ile %96,29 olarak belirlenmiştir. Tespit süreleri açısından değerlendirildiğinde NB algoritmasının atakları tespit süresi 0,01 sn olarak belirlenmiştir.

5. SONUÇLAR VE ÖNERİLER

Çalışma kapsamında, CICDDOS2019 veri seti üzerinde karşılıklı bilgi metodu kullanılarak seçilen öznitelikler ve tüm öznitelikler kullanılarak K-En Yakın Komşu, Karar Ağacı, Naive Bayes ve Rastgele Orman algoritmasının DDoS ataklarını tespit etme performansları karşılaştırılmıştır. Sonuçları genelleştirebilmek için 5 kat çapraz doğrulama yöntemi kullanılarak deneyler gerçekleştirilmiştir.

Veri setinde yer alan verilerde öznitelik seçimi yapılmadan tüm özniteliklerin kullanıldığı DDoS ataklarının tespitinde çoklu sınıflandırma yöntemi kullanıldığında en yüksek doğruluk oranı %99,98 ile KNN ve DT algoritmalarında, en yüksek kesinlik değeri %99,21 ile KNN algoritmasında, en yüksek duyarlılık değeri %98,09 ile KNN algoritmasında, en yüksek F1 puanı %98,65 ile KNN algoritmasında en hızlı sınıflandırma ise 0,03 sn ile DT algoritmasında elde edilmiştir.

Veri setinde yer alan verilerde öznitelik seçimi yapılmadan tüm özniteliklerin kullanıldığı atak olmayan paketlerin tespitinde ikili sınıflandırma yöntemi kullanıldığında en yüksek doğruluk oranı %99,34 ile KNN algoritmasında, en yüksek kesinlik değeri %98,56 ile KNN algoritmasında, en yüksek duyarlılık değeri %97,98 ile KNN algoritmasında, en yüksek F1 puanı %98,27 ile KNN algoritmasında, en hızlı sınıflandırma 0,01 sn ile DT algoritmasında elde edilmiştir.

Veri setinde yer alan verilerde karşılıklı bilgi metodu yardımıyla öznitelik seçimi yapıldığında seçilen öznitelikler ile DDoS ataklarının tespitinde çoklu sınıflandırma yöntemi kullanıldığında en yüksek doğruluk oranı %94,56 ile RF algoritmasında, en yüksek kesinlik değeri %91,49 ile RF algoritmasında, en yüksek duyarlılık değeri %94,56 ile RF algoritmasında, en yüksek F1 puanı %93,00 ile RF algoritmasında, en hızlı sınıflandırma 0,01 sn ile DT ve NB algoritmalarında elde edilmiştir.

Veri setinde yer alan verilerde karşılıklı bilgi metodu yardımıyla öznitelik seçimi yapıldığında seçilen öznitelikler ile atak olmayan paketlerin tespitinde ikili sınıflandırma yöntemi kullanıldığında en yüksek doğruluk oranı %96,29 ile NB algoritmasında, en yüksek kesinlik değeri %93,44 ile RF algoritmasında, en yüksek duyarlılık değeri %92,99 ile RF algoritmasında, en yüksek F1 puanı %93,21 ile RF algoritmasında, en hızlı sınıflandırma 0,003 sn ile DT algoritmasında elde edilmiştir.

CCIDDOS2019 veri seti içinde yer alan DDoS ataklarını tespit etme her bir atak için ayrı ayrı değerlendirme yapıldığında öznitelik seçimi yapıldıktan sonra algoritmalar ikili sınıflandırma metodunda LDAP, SNMP, TFTP, SYN ataklarını tespit ederken daha yüksek

performans göstermişlerdir. Bu atakların ortak yanı protokol tabanlı saldırılar olmalarıdır. Ortak noktaları dikkate alındığından karşılıklı bilgi metodu ile öznitelik seçimi protokol tabanlı DDoS ataklarının sınıflandırılmasında etkin bir ön işleme algoritması olarak kullanılabilir. Atak tespitinde tüm öznitelikler kullanıldığında algoritmaların hepsi veri seti içinde bulunan DDoS ataklarının tümü için yüksek performansa ulaşmıştır ancak tespit süreleri yüksektir. DDoS ataklarının önemli özelliklerinden biri olan hız faktörü dikkate alındığında karşılıklı bilgi metodu kullanılarak gerçekleştirilen öznitelik seçimiyle yapılan sınıflandırma işlemlerinde, atak tespit süresinde pozitif yönde bir düşüş gözlemlenmiştir. Bu durumu göz önünde bulundurduğumuzda karşılıklı bilgi metodu kullanarak öznitelik seçimi gerçekleştikten sonra algoritmaların yüksek performans gösterdiği atak türlerini tespit etmekte kullanılması DDoS ataklarının tespitinde daha avantajlı ve etkili olabilir.

Çalışma kapsamında ele alınan algoritmalar saldırı tespit sistemlerindeki donanımlara entegre edilerek DDoS saldırılarının gerçek zamanlı tespitinde ve gerektiğinde ağ trafiğinin yönlendirilmesinde kullanılabilir.

Karşılıklı bilgi metodu ile yapılan öznitelik seçiminin algoritmaların tespit başarılarında göreceli bir azalmaya neden olurken işlem zamanlarının kısalmasında önemli ölçüde katkı sağladığı gözlenmiştir. Karşılıklı bilgi metodunun kural tabanlı saldırı tespit sistemlerinde yer alan kuralların oluşturulmasında etkin bir şekilde kullanılabileceği değerlendirilmektedir.

Bir diğer yandan teknolojinin hızla ilerlemesine rağmen internet teknolojilerinin her alanı aynı ivmede gelişim gösterememektedir. Dolayısıyla sürekli gelişim göstermekte olan yapay zekâ bir saldırganın elinde siber atak vektörü olarak kullanılabilir. Çalışma çerçevesinde ele alınan yapay zekâ algoritmalarının kullanılması ile elde edilen sonuçlar sadece bu şartlar için geçerlidir. Aynı zamanda henüz ortaya çıkmamış ve çıkma ihtimali olan yeni bir saldırı vektörü ile karşılaşıldığında kullanılan engelleme sistemlerinin başarıları yeniden araştırılmalıdır. Bu olumsuzluğu azaltabilmek için oluşturulacak saldırı tespit sistemlerinin periyodik olarak yeniden eğitilmesi ve güncel tutulması etkili bir saldırı tespit sisteminin kurulmasında önemli bir etken olarak karşımıza çıkmaktadır.

Çalışma kapsamında danışmanlı öğrenme algoritmaları ele alınmıştır. Gelişen teknolojik şartlara göre saldırı türlerinde de farklılaşmalar olması mümkündür. Bu nedenle kullanılan yapay zekâ algoritmasının sürekli güncellenmesi gerekecektir. Oluşturulacak saldırı tespit sistemlerinde kendi kendine öğrenme yapabilecek danışmansız öğrenme algoritmalarının ya da destekleyici öğrenme algoritmalarının kullanılması saldırı tespit sistemlerinin yeni tür atakları tespit etmesinde, daha etkin bir savunma yapısı oluşturulmasına olumlu katkılar sağlayacağı değerlendirilmektedir.

KAYNAKLAR

Aktaş, O., 2018, Siber Güvenlik, Gazi Kitapevi, Ankara, 101-112.

Alkan, M., 2012, Siber güvenlik ve siber savaşlar, *Bilgi Güvenliği Derneği TBMM Internet Komisyonu Sunumu*, Ankara.

Altınkaynak, M., 2017, Siber Güvenlik ve Hacking, Abaküs Yayınevi, İstanbul, 4-78.

Alzahrani, Rami J., ve Ahmed Alzahrani. 2021, Security analysis of ddos attacks using machine learning algorithms in networks traffic, *Electronics* 10(23), p. 2919.

Alzahrani, S. ve Hong, L., 2018, Detection of distributed denial of service (Ddos) attacks using artificial intelligence on cloud, *IEEE World Congress on Services (Services)*, San Francisco, CA, USA, p. 35-36.

Anonim, 2022(a), Cloudflare DDoS threat report for 2022 Q4, *Cloudflare*, [online] <https://blog.cloudflare.com/ddos-threat-report-2022-q4/> [Ziyaret Tarihi: 27.11.2023], Rapor.

Anonim, 2022(b), 2022 in review: DDoS attack trends and insights, *Microsoft Azure*, [online] <https://www.microsoft.com/en-us/security/blog/2023/02/21/2022-in-review-ddos-attack-trends-and-insights/> [Ziyaret Tarihi: 15.12.2023], Rapor.

Anonim, 2023(a), Cisco annuel internet report, *Cisco*, [online] <https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html> [Ziyaret Tarihi: 11.12.2023], Rapor.

Anonim, 2023(b), Spamhaus Botnet Threat Update, *Spamhaus*, [online] <https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q1%20Botnet%20Threat%20Update.pdf> [Ziyaret Tarihi: 19.12.2023], Rapor.

Anonim, 2023(c), DDoS Statistical Report for 1HY 2023 [online], *Nexusguard*, <https://www.nexusguard.com/threat-report/ddos-statistical-report-for-1hy-2023>, [Ziyaret Tarihi: 09.12.2023], Rapor.

Anonim, 2023(d), DDoS threat report for 2023 Q4, *Cloudflare*, [online] <https://blog.cloudflare.com/ddos-threat-report-2023-q4> [Ziyaret Tarihi: 03.01.2024], Rapor.

Archer, K. J., ve Kimes, R. V., 2008. Empirical characterization of random forest variable importance measures. *Computational Statistics & Data Analysis* 52(4), p. 2249–2260.

Asarkaya, S., Kaynar, O., Yelmen, İ., ve Yıldırım, F., 2021, Ddos saldırılarının makine öğrenimi algoritmalarıyla tespiti, *Tasarım Mimarlık ve Mühendislik Dergisi* 1(3), p. 221-232.

Aslanyürek, M., 2016, İnternet ve sosyal medya kullanıcılarının internet güvenliği ve çevrimiçi gizlilik ile ilgili kanaatleri ve farkındalıkları, *Maltepe İletişim Fakültesi Dergisi* 3, p. 80-106.

Aslay, F., 2017, Siber saldırı yöntemleri ve Türkiye'nin siber güvenlik mevcut durum analizi, *International Journal of Multidisciplinary Studies and Innovative Technologies* 1(1), p. 24-28.

Avcı, İ., ve Koca, M., 2023, Predicting ddos attacks using machine learning algorithms in building management systems. *Electronic*, 12(19), p. 4142.

- Aydın, E., 1992, Bilişim Suçları ve Hukukuna Giriş, Doruk Yayınları, Ankara, 234-254.
- Bace, R., ve Mell, P., 2001, Intrusion detection systems, *National Institute of Standards and Technology NIST SP*. 800-31.
- Bahadır, O., ve Türkmençalıkoğlu, H., 2021, Bilgi kuramında shannon entropisi ve uygulamaları, *Avrupa Bilim ve Teknoloji Dergisi* 32, p. 491-497.
- Balcı, B., 2016. Bilgisayar Bilimlerine Giriş, Nobel akademik yayıncılık, İstanbul, p. 340-345.
- Batchu, R. K., ve Seetha, H. 2021. A generalized machine learning model for DDoS attacks detection using hybrid feature selection and hyperparameter tuning. *Computer Networks* 200, p.108498.
- Breiman, L, Friedman, J. H., Olshen, R. A., ve Stone, C. J., 1984. Classification and regression trees. *Biometrics* 40, p. 874.
- Breiman, L., 2001. Random Forests. *Machine Learning* 45(1), p. 5–32.
- Can, Ö., ve Akbaş, M., 2014, Kurumsal ağ ve sistem güvenliği politikalarının önemi ve bir durum çalışması. *TÜBAV Bilim Dergisi* 7(2), p.16-31.
- Cortes, C., ve Vapnik, V., 1995. Support-vector networks, *Machine Learning* 20(3), p. 273–297.
- Czyz, J., Kallitsis, M., Gharaibeh M., Papadopoulos, C., Bailey, M., ve Karir, M., 2014, Taming the 800 pound gorilla: the rise and decline of NTP DDoS attacks. *Proceedings of the Fourteenth ACM Internet Measurement Conference, ACM IMC 2014, Association for Computing Machinery*, p. 435–448.
- Çebi, B. C., Bulut, S., Fırat, F., Karataş, H., ve Şahingöz, K. G., 2019, Saldırı tespit sistemlerinde makine öğrenmesi modellerinin karşılaştırılması, *Erzincan University Journal of Science and Technology* 12(3), p. 1513–1525.
- Çelik, C., ve Bilge, H. Ş., 2015, Ağırlıklandırılmış koşullu karşılıklı bilgi ile öz nitelik seçimi, *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi* 30, p. 4.
- Çelik, H. E., Korkmaz, D., ve Kapar, M., 2018, Sınıflandırma ve regresyon ağaçları ile rastgele orman algoritması kullanarak botnet tespiti, Van Yüzüncü Yıl Üniversitesi, *Yüzüncü Yıl Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, 23(3), p. 297–307.
- Çelik, Ş., 2012, Stuxnet saldırısı ve SBD'nin siber savaş stratejisi: uluslararası hukukta kuvvet kullanmaktan kaçınma ilkesi çerçevesinde bir değerlendirme, *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*. 15(1), p. 137-75.
- Çil, A. E., 2021, Ddos saldırılarının tespiti ve sınıflandırılması için derin öğrenme modeli, *Marmara Üniversitesi Fen Bilimleri Enstitüsü*, Yüksek Lisans Tezi, İstanbul.
- Çil, A. E., Yıldız, K., ve Buldu, A., 2021, Detection of DDoS attacks with feed forward based deep neural network model, *Expert Systems with Applications* 169(4), p. 114520.
- Das, S., Venugopal, D., Shiva, S., ve Sheldon, F. T., 2020. Empirical evaluation of the ensemble framework for feature selection in DDoS attack, *In Proceedings. 2020 7th IEEE International*

Conference on Cyber Security and Cloud Computing and 2020 6th IEEE International Conference on Edge Computing and Scalable Cloud, CSCloud EdgeCom, p. 56-61.

Dasari, K. B., ve Devarakonda, N., 2021, Detection of different DDoS attacks using machine learning classification algorithms, *Ingenierie Des Systemes d'Information* 26(5), p. 461–468.

Deshmukh, R., ve Devadkar, K., 2015, Understanding DDoS attack & its effect in cloud environment. *Procedia Computer Science* 49, p. 202-210.

Doriguzzi, C. R., Millar, S., Scott-Hayward, S., Martinez-Del-Rincon, J., ve Siracusa, D., 2020, Lucid: a practical lightweight deep learning solution for DDoS attack detection, *IEEE Transactions on Network and Service Management*, 17(2).

Elsayed, M. S., Le-Khac, N. A., Dev, S., ve Jurcut, A., D., DDoSNet: a deep-learning model for detecting network attacks, 2020, *2020 IEEE 21st International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)*, Cork, Ireland, p 391-396,

Estevez, P. A., Tesmer, M., Perez C. A., ve Zurada, J. M., 2009, ormalized mutual information feature selection, *IEEE Transactions on Neural Networks* 20(2), p. 189-201.

Fan, G. F., Guo, Y. H., Zheng, J. M., ve Hong, W. C., 2019, Application of the weighted k-nearest neighbor algorithm for short-term load forecasting, *Energies*, 12(5).

Farid, D. M., ve Rahman, M. Z., 2010, Anomaly network intrusion detection based on improved self adaptive Bayesian algorithm. *Journal of Computers*, 5(1).

Fawcett, T., 2006, An introduction to ROC analysis, *Pattern Recognition Letters* 27(8), p. 861–874.

Gezgin, D. M., ve Buluş, E., 2013. Kablosuz Ağlar için bir DoS Saldırısı Tasarımı. *Bilişim Teknolojileri Dergisi* 6(3), p. 17-23.

Gondim, J., Albuquerque, R., ve Sandoval Orozco, A., 2020, Mirror saturation in amplified reflection Distributed Denial of Service: A case of study using SNMP, SSDP, NTP and DNS protocols. *Future Generation Computer Systems* 108, p. 68-81.

Gu, Q., ve Liu, P., 2012, Denial of service attacks. *In Handbook of Computer Networks* 3, p. 454-468.

Gürel, A., ve Yalçinkaya, M. A., 2021, Siber Güvenlik, 1. Basım, Dikeyksen Yayınevi, İstanbul, 23-41.

Gürsakar, N., 2018. Makine Öğrenmesi, Dora Yayınları, Bursa, 67-71.

Hatipoğlu, C., ve Tunacan, T., 2021. Türkiye’de siber saldırı ve tespit yöntemleri: bir literatür taraması. *Bilecik Şeyh Edebalı Üniversitesi Fen Bilimleri Dergisi*, 8(1), p. 430-445.

Hassan, D., 2017, Cost-Sensitive Access control for detecting remote to local (R2L) and user to root (U2R) attacks, *International Journal of Computer Trends and Technology (IJCTT)* 43(2), p. 124-129.

Jabbar M. A., Deekshatulu, B., ve Chandra, P., 2013, Classification of heart disease using k-nearest neighbor and genetic algorithm. *Procedia Technology* 10, p. 85–94.

- Kaya, Ö. F., ve Öztürk, E., 2017, Veri ve ağ güvenliği için uygulama ve analiz çalışmaları. *İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi* 16(31), p. 85-102.
- Kaya, Ç., ve Yıldız, O., 2014, Makine öğrenmesi teknikleriyle saldırı tespiti: Karşılaştırmalı analiz, *Marmara University Journal of Science*, 26(3).
- Kaypak, Ş., 2013, Çevresel güvenlik ve sınır aşan çevre suçları, *Dumlupınar Üniversitesi, Sosyal Bilimler Dergisi* (38).
- Khuphiran, P., Leelaprute, P., Uthayopas, P., Ichikawa, K., ve Watanakesuntorn, W., 2018, Performance comparison of machine learning models for DDoS attacks detection, *22nd International Computer Science and Engineering Conference (ICSEC)*.
- Kırbaş, K., 2021, Sistem ve Network Mühendisliği, Kodlab Yayınevi, İstanbul, 71-102.
- Kishore, D., ve Devarakonda, Na., 2021, Detection of Different DDoS Attacks Using Machine Learning Classification Algorithms. *Ingénierie des systèmes d'information*. (26), p. 461-468.
- Kochetkova, K., 2016. How to not break the Internet. [online] <https://www.kaspersky.com/blog/attack-on-dyn-explained/13325/>[Ziyaret Tarihi: 12.11.2023].
- Koyuncu, M. D., ve Ünlü, N., 2022., Yapay zekâ tekniklerinin saldırı tespit sistemleri'nde kullanımı. *Beykoz Akademi Dergisi* 10(1), p. 78-87.
- Kumar, D., Pateriya, R. K., Gupta, R. K., Dehalwar, V., ve Sharma, A., 2023, DDoS detection using deep learning, *Procedia Computer Science* 218, p. 2420-2429.
- Kumari, K., ve Mrunalini, M., 2022, Detecting denial of service attacks using machine learning algorithms. *J Big Data* 9, p. 56.
- Kurt, A., Buldu, B., ve Cedimoğlu, İ. H., 2020, Xgboost ve rastgele orman algoritmalarının ağ tabanlı saldırı tespitine yönelik performanslarının karşılaştırılması, *International Marmara Sciences Congress*, p. 730-736.
- Kushwah, G. S., ve Ranga, V., 2021, Optimized extreme learning machine for detecting DDoS attacks in cloud computing, *Computers and Security*, p. 105.
- Learned-Miller, E. G., 2013, Entropy and mutual information, *University of Massachusetts, Amherst, Department of Computer Science*, p. 4.
- Liao, H. J., Richard Lin, C. H., Lin, Y. C., ve Tung, K. Y., 2013, Intrusion detection system: a comprehensive review, *Journal of Network and Computer Applications* 36(1), p. 16-24.
- Loh, W. Y., ve Shih, Y. S., 1997, Split selection methods for classification trees, *Statistica Sinica* 7(4), p. 815-840.
- Ma, R., Wang, Q., Bu, X., ve Chen, X., 2023, Real-Time detection of DDoS attacks based on Random Forest in SDN, *Applied Sciences* 13(13), p. 7872.
- Mandle, H., ve Fischer, F., 2001, Computer networking for education, *International Encyclopedia of the Social & Behavioral Science*, p. 2470-2473.
- Manjula, H. T., ve Mangla, N., 2021, An approach to on-stream DDoS blitz detection using machine learning algorithms, *Materials Today: Proceedings* 80(3), p. 3492-3499.

- Mistry, A. G., 2023, Intrusion detection classification using machine learning, *California state university san marcos*, Yüksek Lisans Tezi.
- Mirkovic, J., Prier G., ve Reiher, P., 2002, Attacking DDoS at the source, *10th IEEE International Conference on Network Protocols, Proceedings*, Paris, France, p. 312-321.
- Mountrakis, G., Im, J., ve Ogole, C., 2011, Support vector machines in remote sensing: a review, *ISPRS Journal of Photogrammetry and Remote Sensing*, 66(3), p. 247-259.
- Mudzingwa, D., ve Agrawal, R., 2012, A study of methodologies used in intrusion detection and prevention system (IDPS). *Proceedings of IEEE Southeastcon*, p. 1-6.
- Nicholson, P., 2022, Five most famous ddos attacks and then some, from five most famous ddos attacks and then some [online] <https://www.a10networks.com/blog/5-most-famous-ddos-attacks/> [Ziyaret Tarihi: 9.10.2023]. Rapor.
- Putri, D., Kristiyanti, D., Indrayuni, E., Nurhadi, A., ve Hadinata, D., 2020), Comparison of naive bayes algorithm and support vector machine using pso feature selection for sentiment analysis on e-wallet review. *Journal of Physics: Conference Series* 1641(1), p. 012085.
- Raj, R., ve Kang, S. S., 2022, Mitigating ddos attack using machine learning approach in SDN, *2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*, Greater Noida, India, p. 462-467.
- Rijswijk-Deij, R., Sperotto, A., ve Pras, A., 2014, DNSSEC and its potential for DDoS attacks: a comprehensive measurement study. *Proceedings of the Fourteenth ACM Internet Measurement Conference, ACM IMC 2014, Association for Computing Machinery*, p. 449-460.
- Rish, I., 2001, An empirical study of the naïve bayes classifier. *IJCAI 2001 Workshop Empirical Methods in Artificial Intelligence*, p. 41-46.
- Salunkhe, H., Jadhav, S., ve Bhosale, V.H., 2017, Analysis and review of TCP SYN Flood attack on network with its detection and performance metrics. *International Journal of Engineering Research and Technology (IJERT)* 6(1).
- Sambangi, S., ve Gondi, L., 2020, A machine learning approach for DDoS (Distributed Denial of Service) attack detection using Multiple Linear Regression, *Proceedings* 63(1), p. 51.
- Santhosh, S., Sambath M., and Thangakumar, J., 2023, Detection Of DDOS Attack using machine learning models, *2023 International Conference on Networking and Communications (ICNWC)*, Chennai, India, p. 1-6.
- Saini, P. S., Behal, S., ve Bhatia, S., 2020, Detection of DDoS attacks using machine learning algorithms, *7th International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, India, p. 16-2.
- Sazzadul, H. M., 2012, An implementation of intrusion detection system using genetic algorithm, *International Journal of Network Security & Its Applications*, 4(2).
- Scarfone, K., ve Mell, P., 2007, Guide to intrusion detection and prevention systems (IDPS), *NIST Special Publication*, 800-94.

- Sharafaldin, I., Lashkari, A. H., Hakak, S., ve Ghorbani, A. A., 2019, Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy, In *Proceedings-International Carnahan Conference on Security Technology*, p.1-8.
- Sharma, A., ve H. Babbar., 2023, Evaluation and Analysis: Internet of things using machine learning algorithms for detection of DDoS attacks, *2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE)*, Bengaluru, India, p. 1203-1208.
- Shawe-Taylor, J., ve Sun, S., 2014, Kernel methods and support vector machines. In *Academic Press Library in Signal Processing 1*, p. 857-881.
- Shroff, J., Walambe, R., Singh, S. K., ve Kotecha, K., 2022, Enhanced security against volumetric ddos attacks using adversarial machine learning, *Wireless Communications and Mobile Computing*, p. 1-10.
- Sieklik, B., Macfarlane, R., ve Buchanan, W. J., 2016, Evaluation of TFTP DDoS amplification attack, *Computer & Science 57*, p. 67-92.
- Sunita, S., Paul, A. M., Parth, S., ve Moin, K., 2020 Detection of application layer DDoS attacks using big data technologies, *Journal of Discrete Mathematical Sciences and Cryptography 23(2)*, p. 563-571.
- Specht, S., ve Lee, R., 2003, Taxonomies of distributed denial of service networks, attacks, tools and countermeasures, *Journal of Information Security 4*, p. 3.
- Stiawan, D., Suryani, M., Susanto, S., Idris, Y., Aldalaien, M., Alsharif, N., ve Budiarto, R., 2021, Ping flood attack pattern recognition using a k-means algorithm in an internet of things (iot) network. *IEEE Acces*, p. 1-1.
- Şamlıoğlu, H., 2021, DDoS saldırıları ve türleri, *Privia Cyber Security Consulting*, İstanbul.
- Taner, C., 2017, Ağ yöneticiliğinin temelleri, Abaküs Yayınevi, İstanbul, 1-46,
- Thorat, O., Parekh, N., ve Mangrulkar, R., 2021, TaxoDaCML: Taxonomy based Divide and Conquer using machine learning approach for DDoS attack classification, *International Journal of Information Management Data Insights*, 1(2), p. 100048.
- Toprak, H., 2021, Akıllı saldırı tespit sistemleri, *Batman Üniversitesi Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi*.
- Toprak A., Yıldırım E. A., Binark F. M., Çomu T., Senem B., ve Aygöl E., 2009, Toplumsal paylaşım ağı Facebook görüldüğüm öyleyse varım. *Kalkedon Yayınları*, İstanbul, 1-13.
- Turhan, O., 2006, Bilgisayar ağları ile ilgili suçlar (Siber Suçlar), *T.C Başbakanlık Devlet Planlama Müsteşarlığı Hukuk Müşavirliği: Planlama Uzmanlığı Tezi*, Ankara.
- Türkyılmaz, Y., ve Şentürk, A., 2022, Saldırı tespitinde makine öğrenmesi yöntemlerinin performans analizi. *European Journal of Science and Technology (32)*, p. 107-112.
- Uçak, K., 2012, Destek vektör regresyonu ile pid kontrolör tasarımı, *İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi*.
- Ullman, R. H., 1983, Redefining Security, *International Security*, 8(1), p. 129–153.

Wang, L., 2019, Research and implementation of machine learning classifier based on KNN. *In IOP Conference Series: Materials Science and Engineering Vol. 677*, No. 5, p. 052038.

Warburton, D., 2021, DDoS attack trends for 2021 [online] <https://www.f5.com/labs/articles/threat-intelligence/ddos-attack-trends-for-2020> [Ziyaret Tarihi: 27.12.2023], Rapor.

Ware, H. W., 1967, Security and privacy copmuter system, *Presented at the Spring Joint Computer Conference*, p. 3544.

Wickramasinghe, I., ve Kalutarage, H., 2021, Naive Bayes: applications, variations and vulnerabilities: a review of literature with code snippets for implementation Indika, *Soft Computing*, 25(3), p. 2277-2293.

Winder, D., 2019, Recording data for cyberdefence [online] <https://www.brookcoursolutions.com/recording-data-for-cyberdefence/> [Ziyaret Tarihi 10.10.2023], Rapor.

Wroblewski, M. H., ve Hens, M. K., 1990, Introduction to Law Enforcement and Criminal Justice, *Third Edition*, p. 132-143.

Vergara, J., ve Estevez, P., 2014, A review of feature selection methods based on mutual information, *Neural Computing and Applications* 24(1), 175-186.

Verma, P., Anwar, S., Khan, S., ve Mane, S. B., 2018, Network intrusion detection using clustering and gradient boosting, *9th International Conference on Computing, Communication and Networking Technologies (ICCCNT) IEEE*, p. 1-7.

Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., ve Venkatraman, S., 2019, Deep learning approach for intelligent intrusion detection system. *IEEE Access* 7, p. 41525–41550.

Yazıcıoğlu Y., 2004, Bilişim suçları konusunda 2001 Türk Ceza Kanunu tasarısının değerlendirilmesi, *Hukuk ve Adalet: Eleştirel Hukuk Dergisi* 1(1), İstanbul.

Ye, J., Cheng, X., Zhu, J., Feng, L., ve Song, L., 2018, A DDoS attack detection method based on SVM in software defined network, *Security and Communication Networks*, p. 1-8.

Yeniman Yıldırım, E., 2018, Bilişim sistemlerine yönelik siber saldırılar ve siber güvenliğin sağlanması. *Mesleki Bilimler Dergisi (MBD)* 7(2), p. 24-33.