

**KARADENİZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ**

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

SCADA SİSTEMLERİ İÇİN MAKİNE ÖĞRENİMİ TABANLI HATA TESPİTİ

YÜKSEK LİSANS TEZİ

Tolgahan ÖZTÜRK

**OCAK 2023
TRABZON**



KARADENİZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

SCADA SİSTEMLERİ İÇİN MAKİNE ÖĞRENİMİ TABANLI HATA TESPİTİ

Tolgahan ÖZTÜRK

ORCID : - - -

Karadeniz Teknik Üniversitesi Fen Bilimleri Enstitüsünde
"BİLGİSAYAR YÜKSEK MÜHENDİSİ"
Unvanı Verilmesi İçin Kabul Edilen Tezdir.

Tezin Enstitüye Verildiği Tarih : 02 / 12 / 2022

Tezin Savunma Tarihi : 02 / 01 / 2023

Tez Danışmanı : Prof. Dr. Cemal KÖSE
ORCID : - - -

Trabzon 2023

ÖNSÖZ

İnsan nüfusu hızla artmaktadır. İnsan nüfusunun artması, insanların ihtiyaçlarının da artması anlamına gelmektedir. Artan bu ihtiyaçları karşılamakta oldukça zor bir durumdur. Teknolojinin hızla gelişmesi, birçok farklı alanda kullanılıyor olması ve sunduğu faydalar ile insanlar açısından bu zorluğu aşmada çok büyük bir öneme sahip olmaktadır.

Teknolojinin gelişmesiyle birlikte artık çevremizde akıllı sistemler ve bu sistemlere bağlı akıllı cihazlar ortaya çıkmaktadır. Bu akıllı cihazlar endüstrinin bütün alanlarında kullanılmaktadır. Uzaktan yönetilebilir olmaları ve ihtiyaçlara çok daha hızlı cevap verebilmelerinden dolayı çok daha fazla tercih edilmektedirler.

Bu akıllı sistemlerin ve bu akıllı sistemlere bağlı cihazların her ne kadar faydaları olsa da çok önemli ve dikkat çekici konulardan birisi de güvenlik sorunudur. Akıllı sistemlerin ve akıllı cihazların yaşadığı en büyük ve en yaygın güvenlik sıkıntıları ise siber saldırılardır. Bu nedenle bu siber saldırıların en hızlı şekilde tespit edilmesi ve saldırı türlerinin tespit edilerek buna göre önlem alınması çok önemli bir konu olmaktadır.

Bu çalışmada güvenlik sisteminin performansının iyileştirilmesi için SCADA sistemlerinde farklı saldırı türlerinin sınıflandırılması sorunu üzerinde durulmuştur. Bu kapsamda sınıflandırma probleminde 5 farklı makine öğrenmesi algoritması gerçekleştirilmiş ve bu algoritmaların performansı detaylı olarak tartışılmıştır. Ayrıca örnek veri seti için kullanılan makine öğrenmesi yaklaşımlarının zaman gereksinimi performansı da analiz edilmiştir.

Çalışmalarım süresince bilgi, görüş ve önerileriyle bana yardımcı olan çok değerli danışman hocam Sayın Prof. Dr. Cemal Köse'ye teşekkürlerimi bir borç bilir ve şükranlarımı sunarım.

Yüksek lisans eğitimim süresince sabır, destek ve sevgisiyle hep yanımda olan değerli eşime, bu yaşıma kadar benim her anımda yanımda olan ve desteklerini hiçbir zaman esirgemeyen canım aileme ve çalışmalarımda her zaman bana destek olan değerli hocalarım Dr. Öğr. Üyesi Zeynep Turgut Akgün, Dr. Öğr. Üyesi Gökçe Akgün'e teşekkür eder şükranlarımı ve saygılarımı sunarım.

Tolgahan ÖZTÜRK

Trabzon 2023

TEZ ETİK BEYANNAMESİ

Yüksek Lisans Tezi olarak sunduğum “SCADA Sistemleri İçin Makine Öğrenimi Tabanlı Hata Tespiti” başlıklı bu çalışmayı baştan sona kadar danışmanım Prof. Dr. Cemal KÖSE’nin sorumluluğunda tamamladığımı, verileri / örnekleri kendim topladığımı, deneyleri / analizleri ilgili laboratuvarlarda yaptığımı / yaptırdığımı, başka kaynaklardan aldığım bilgileri metinde ve kaynakçada eksiksiz olarak gösterdiğimi, çalışma sürecinde bilimsel araştırma ve etik kurallara uygun olarak davrandığımı ve aksinin ortaya çıkması durumunda her türlü yasal sonucu kabul ettiğimi beyan ederim. 02/01/2023

Tolgahan ÖZTÜRK

İÇİNDEKİLER

	<u>Sayfa No</u>
ÖNSÖZ	I
TEZ ETİK BEYANNAMESİ.....	II
İÇİNDEKİLER.....	III
ÖZET	V
SUMMARY	VI
ŞEKİLLER DİZİNİ.....	VII
TABLolar DİZİNİ.....	IX
SEMBOLLER DİZİNİ	X
1. GENEL BİLGİLER.....	1
1.1 SİBER GÜVENLİK	1
1.1.1. Siber Fiziksel Sistemler	1
1.1.2. Siber Tehdit	4
1.1.3. Siber Saldırı	5
1.1.4. Siber Saldırı Türleri	6
1.1.4.1. Man-In-The-Middle (MITM) Saldırısı.....	7
1.1.4.2. ARP Poisoning	9
1.1.4.3. DoS ve DDoS Saldırıları	11
1.1.4.4. TCP Flood	13
1.1.4.5. ICMP Flood	15
1.1.4.6. Land Attack	16
1.1.4.7. Scanning Attack.....	18
1.1.4.7.1. SYN Scan	20
1.1.4.7.2. FIN Scan	21
1.1.4.7.3. Null Scan	21
1.1.4.7.4. XMAS Scan.....	21
1.1.5. Saldırı Tespit ve Önleme Sistemleri.....	22
1.1.5.1. Saldırı Tespit Sistemleri	23
1.1.5.2. Saldırı Önleme Sistemleri.....	25
1.1.6. Mevcut Çalışmalar.....	28

1.1.7.	Denetim Kontrolü ve Veri Toplama Sistemi	33
1.1.7.1.	Denetim Kontrolü ve Veri Toplama Sisteminin Yapısı	34
1.1.7.2.	Denetim Kontrolü ve Veri Toplama Sisteminin İşlevleri.....	38
1.1.7.3.	Denetim Kontrolü ve Veri Toplama Sisteminin Uygulama Alanları.....	38
1.1.7.4.	Denetim Kontrolü ve Veri Toplama Versiyonları	40
1.1.7.5.	Denetim Kontrolü ve Veri Toplama Sistemi Açısından Tehditler	43
1.1.7.6.	Denetim Kontrolü ve Veri Toplama Sistemi Açısından Saldırıları.....	44
1.1.8.	Bilgi Teknoloji Sistemler ve Denetim Kontrolü ve Veri Toplama Sistemlerinin Kıyaslanması	45
1.1.8.1	Performans ve Zamanlama Gereksinimlerine Göre Kıyaslama	46
1.1.8.2.	Kullanılabilirlik Gereksinimlerine Göre Kıyaslama.....	47
2.	YAPILAN ÇALIŞMALAR.....	48
2.1.	Kullanılan Veri Kümesi.....	48
2.2.	Çalışmada Kullanılan Yöntemler	50
2.2.1.	Makine Öğrenmesi	50
2.2.1.1.	K-En Yakın Komşu (K-Nearest Neighbors-KNN) ile Sınıflandırma.....	52
2.2.1.2.	Destek Vektör Makinesi (Support Vector Machine - SVM) ile Sınıflandırma....	55
2.2.1.3.	Karar Ağacı (Decision Tree) ile Sınıflandırma.....	57
2.2.1.4.	Rastgele Orman (Random Forest) ile Sınıflandırma	60
2.2.1.5.	AdaBoost (Adaptive Boosting) ile Sınıflandırma	62
3.	BULGULAR	64
4.	SONUÇLAR VE TARTIŞMA.....	70
5.	ÖNERİLER.....	77
6.	KAYNAKLAR.....	78
7.	ÖZGEÇMİŞ	

Yüksek Lisans Tezi

ÖZET

SCADA SİSTEMLERİ İÇİN MAKİNE ÖĞRENİMİ TABANLI HATA TESPİTİ

Tolgahan ÖZTÜRK

Karadeniz Teknik Üniversitesi

Fen Bilimleri Enstitüsü

Bilgisayar Mühendisliği Anabilim Dalı

Danışman: Prof. Dr. Cemal KÖSE

2023, 87 Sayfa

Enerji dağıtım sistemleri ve Siber-Fiziksel Sistemler, bilgi teknolojisi açısından çok önemli bir yere sahiptir. Bilgi teknolojisinin bu alanlarda kullanılması aynı zamanda bir risk oluşturmaktadır. Bu sistemler içerisinde kullanılan SCADA sistemleri gelecek zamanlarda IoT cihazlarıyla iletişim kurabilen bulut tabanlı sistemler haline gelecektir. Fakat SCADA her geçen zaman içinde epeyce saldırı riski taşımaktadır. Buna bağlı olarak hem bu saldırıların tespit edilmesi hem de önlenmesi çok büyük bir önem taşımaktadır.

Bu tez çalışmasında Siber-Fiziksel Sistemlerdeki, SCADA sistemine karşı makine öğrenmesi algoritmaları kullanılarak saldırı tehditlerinin tespiti ve sınıflandırılması yapılmaktadır. Bu sınıflandırma yapılırken her bir saldırı türüne bir eşsiz değer ataması yapılmıştır. Yapılan bu çalışmada saldırı tespiti yapıldığı gibi bu eşsiz değer ataması ile yapılan saldırının tipi de tespit edilmektedir. Saldırı tespitinin yapılması, tipinin belirlenmesi ve performans sonuçları test ortamında gerçekleştirilmiş ve sonuçlar elde edilmiştir.

Anahtar Kelimeler: IOT, Saldırı Tespit Sistemleri, SCADA, Yapay Zekâ,

Master Thesis

SUMMARY

MACHINE LEARNING BASED INTRUSION DETECTION FOR SCADA
SYSTEMS

Tolgahan ÖZTÜRK

Karadeniz Technical University
The Graduate School of Natural and Applied Sciences
Computer Engineering Graduate Program
Supervisor: Prof. Dr. Cemal KÖSE
2023, 87 Pages

Energy distribution systems and Cyber-Physical Systems have a very important place in terms of information technology. The use of information technology in these areas also poses a risk. SCADA systems used in these systems will become cloud-based systems that can communicate with IoT devices in the future. But SCADA carries quite a risk of attack over time. Therefore, both the detection and prevention of these attacks are of great importance.

In this thesis, attack threats are detected and classified using machine learning algorithms against SCADA systems in Cyber-Physical Systems. While making this classification, a unique value is assigned to each attack type. In this study, as well as attack detection, the type of attack is determined with this unique value assignment. Detection of the attack, determination of its type and performance results were carried out in the test environment and the results were obtained.

Keywords: IOT, Intrusion Detection Systems, SCADA, Artificial Intelligence

ŞEKİLLER DİZİNİ

Sayfa No

Şekil 1.1.1. Siber fiziksel sistemler	3
Şekil 1.1.2. Siber tehditler ve bunların algılanması.....	4
Şekil 1.1.4. Siber saldırı türleri genel görünümü.....	7
Şekil 1.1.4.1. MITM saldırısı temsili görüntü	8
Şekil 1.1.4.2. ARP zehirlenmesi saldırısı görüntüsü	11
Şekil 1.1.4.3. Köle bilgisayarların (Zombi, Botnet) görünümü.....	12
Şekil 1.1.4.4. TCP flood saldırısı görüntüsü	14
Şekil 1.1.4.5. ICMP flood saldırı görüntüsü.....	16
Şekil 1.1.4.6. Land saldırısı temsili görüntü.....	17
Şekil 1.1.4.7. Scanning attack görüntüsü	19
Şekil 1.1.4.8. Nmap Çalışma Zamanı Görüntüsü	20
Şekil 1.1.5. Saldırı tespit ve önleme sistemleri genel sınıflandırma.....	23
Şekil 1.1.5.1. Saldırı tespit sistemi çalışma görüntüsü	24
Şekil 1.1.5.2. Saldırı önleme sistemi örnek görüntü.....	26
Şekil 1.1.5.3. Saldırı önleme sistemleri genel görüntüsü	27
Şekil 1.1.7. SCADA yazılım uygulama örnek görüntüsü	34
Şekil 1.1.7.1. SCADA katman yapısı ile temsil edilmesi.....	35
Şekil 1.1.7.2. Modern SCADA sistemi	37
Şekil 1.1.7.3. SCADA sisteminin başlıca uygulama alanları	39
Şekil 1.1.7.4.1. SCADA sisteminin birinci nesil versiyonu	40
Şekil 1.1.7.4.2. SCADA sisteminin ikinci nesil versiyonu	41
Şekil 1.1.7.4.3. SCADA sisteminin üçüncü nesil versiyonu	42
Şekil 1.1.7.4.4. SCADA sisteminin dördüncü nesil versiyonu	43
Şekil 2.2.1.1. KNN algoritması örnek yapısı.....	53
Şekil 2.2.1.2. İki boyutlu destek vektör makinesi örnek uzayı.....	56
Şekil 2.2.1.3. İkili karar ağacı yapısı temsili görüntü.....	58
Şekil 2.2.1.4. Random Forest temsili görüntü	60
Şekil 3.1. K-En Yakın Komşuluk Algoritması (K-Nearest Neighbors-KNN).....	65
Şekil 3.2. Destek Vektör Makinesi (Support Vector Machine-SVM).....	66
Şekil 3.3. Karar Ağacı Algoritması (Decision Tree).....	67

Şekil 3.4. Rastgele Orman Algoritması (Random Forest).....	68
Şekil 3.5. AdaBoost Algoritması (Adeptive Boosting)	69
Şekil 4.1. Karmaşıklık Matrisi (Confusion Matrix)	72
Şekil 4.2. Makine öğrenmesi algoritmalarının genel sonuçları	73



TABLolar DİZİNİ

Tablo 1.1.4.3. DoS ve DDoS saldırılarının karşılaştırılması.....	13
Tablo 1.1.5.2. IPS yapısının algılama mekanizmaları.....	27
Tablo 2.2. Veri setinin özelliklerinin açıklanması.....	48
Tablo 2.2.1.1. KNN sınıflandırma sonuçları.....	54
Tablo 2.2.1.2. SVM sınıflandırma sonuçları.....	57
Tablo 2.2.1.3. Decision Tree sınıflandırma sonuçları.....	59
Tablo 2.2.1.4. Random Forest sınıflandırma sonuçları.....	61
Tablo 2.2.1.5. AdaBoost sınıflandırma sonuçları.....	63
Tablo 4.1. Literatür çalışma sonuçları.....	76

SEMBOLLER DİZİNİ

ACK	Acknowledge (ACK Mesajı)
AD	Anomaly Based Detection (Anormallik Tabanlı Tespit)
AIDS	Application Intrusion Detection System (Uygulama Tabanlı Saldırı Tespit Sistemi)
ARP	Address Resolution Protocol (Adres Çözümleme Protokolü)
BT	Bilgi Teknolojisi
CERT	Danışma Belgesi
CISCO	Network Şirketi
CPU	Central Process Unit (Merkezi İşlem Birimi)
CRC	Cycle Redundancy Check (Döngüsel Artıklık Kontrolü)
DDoS	Denial Of Service Attack (Dağıtılmış Hizmet Reddi)
DL	Deep Learning (Derin Öğrenme)
DNS	Domain Name System (Alan Adı Sistemi)
DoS	Denial of Service (Servis Hizmet Reddi)
GSM	Global System for Mobile Communications (Mobil İletişim İçin Küresel Sistem)
HIDS	Host Intrusion Detection System (Host Tespit Sistemi)
HMI	Human Machine Interface (İnsan Makine Arayüzü)
HTML	Hypertext Markup Language (Hiper Metin İşaretleme Dili)
HTTP	Hyper Text Transfer Protocol (Hiper Metin Transfer Protokolü)
ICMP	Internet Control Message Protocol (İnternet Kontrol Mesaj Protokolü)
IDS	Intrusion Detection System (Saldırı Tespit Sistemi)
IOS	Iphone Operating System (Iphone İşletim Sistemi)
IoT	Internet Of Things (Nesnelerin İnterneti)
IP	Internet Protocol (İnternet Protokolü)
IPS	Intrusion Prevention System (Saldırı Önleme Sistemi)
LAN	Local Area Network (Yerel Alan Ağı)
LAND	Local Area Network Denial (Yerel Alan Ağı Reddi)

MAC	Media Access Control (Ortam Eriřim Kontrolü)
MITM	Man In The Middle (Ortakdaki Adam Saldırısı)
ML	Machine Learning (Makine Öğrenmesi)
MODBUS	Açık Kaynaklı Protokol
NIDS	Network Intrusion Detection System (Ağ Saldırı Tespit Sistemi)
OMRON	Otomasyon ve Tıbbi Cihazlar Üreticisi
PIDS	Protocol Based Intrusion Detection System (Protokol Tabanlı Saldırı Tespit Sistemi)
PLC	Programmable Logic Controllers (Programlanabilir Lojik Kontrol)
RC	Remote Control (Uzaktan Kontrol)
RTU	Remote Terminal Unit (Uzak Terminal Birimi)
SCADA	Supervisory Control and Data Acquisition (Denetim Kontrolü ve Veri Toplama Sistemi)
SD	Signature Based Detection (İmza Tabanlı Tespit)
SFS	Siber Fiziksel Sistemler
SLT	Statistical Learning Theory (İstatistiksel Öğrenme Teorisi)
SPA	Stateful Protocol Analysis (Durum Bilgi Protokol Analizi)
SSL	Secure Sockets Layer (Taşıma Katmanı Güvenliğı)
SYN	Synchronize (Senkronizasyon)
TCP	Transmission Control Protocol (İletim Kontrol Protokolü)
UDP	User Datagram Protocol (Kullanıcı Veri Bloğı Protokolü)
VPN	Virtual Private Network (Sanal Özel Ağ)

1.GENEL BİLGİLER

1.1. Siber Güvenlik

Siber güvenlik; donanımsal araçları, yazılımsal uygulama yapılarını, ağları ve sonuçları (verileri) ifaden eden bir yapıdır. Buna ek olarak siber güvenlik yapısı farklı siber saldırılara karşı güvende tutmak için oluşturulmuş teknoloji yapılarını, uygulamaları ve zamanları açıklayan bir yapıdır. Bilgi teknolojileri güvenliği bu yapının bir tanımı olarak gösterilebilir. Bu nedenle siber güvenliğin amacını yazılım uygulamalarını, ağları ve bilgisayarları oluşması muhtemel siber saldırıya karşı korumayı hedeflemektedir. Daha önce ortaya çıkmış olan siber saldırılara bakıldığında ise birçoğunun yetkisiz erişim, önemli bilgiyi değiştirme veya ortadan kaldırma, saldırının gerçekleştirildiği şahıs ve kurumlardan maddi kazanç elde etme biçiminde görülmektedir.

Siber güvenlik detaylı bir şekilde incelendiğinde organizasyonların tamamını, siber çevre içerisindeki bütün yapıları ve değerli varlıkları korumak için uygulaması yapılan prosedürler, araçlar, güvenlik yapıları, güvenlik tedbirleri, rehberler, risk yönetimi yaklaşımları, eğitimler, sigorta, aksiyonlar ve bütün teknoloji yapılarının birleşmesiyle oluşan bir yapı olarak tanımlanmaktadır.

Siber çevre içindeki bütün yapılara ait bilgi teknoloji yapılarının yapılan saldırılara karşı koruma altına alınması çok önemlidir. Çünkü bilgilerin gizliliğinin ve bütünlüğünün korunmasına ek olarak erişilebilir olarak da devam ettirilmesi için saldırıların belirlenmesi gerekmektedir [1].

1.1.1. Siber Fiziksel Sistemler

Bilgi işlem teknoloji yapı ve sistemleri, siber fiziksel sistemlerle beraber bilgisayarın temel alındığı bir yapı olarak tanımlanabilmektedir. Bunun yanında kablosuz bir bağlantı yapısında ve etkileşim içinde olduğu servis yapıları, iş fonksiyonları ve ortaya çıkan bütün zamanların oluşturduğu bir siber uzay olarak tanımlanabilmektedir.

Siber fiziksel sistemler (SFS), fiziksel dünya ve onun devamındaki zamanların yoğun bir şekilde kullanıldığı ve buna ek olarak verilerin işleme uğramaları ve ulaşılmalarıyla aynı

zamanda da buradaki yer alan servis yapılarının internetle kullanıldığı ortak bir şekilde çalışan hesaplama yapıları olarak açıklanabilmektedir [1,2].

Siber fiziksel sistemlerin uygulamalarında veri direkt olarak algılayıcı sistemler tarafından ölçülebilir veya kontrol üniteleri adı verilen araçlardan elde edilebilir [3,4]. Siber fiziksel sistemler (SFS) aktüatör araçları ve sensör yapılarıyla gerçek olmayan yani sanal bilgi işlem dünyasını ve fiziksel dünyayı birbirine bağlamaktadır. Bu sistemler iki önemli etkenden oluşur. Bunlardan ilki birbirleriyle ataması yapılmış bir internet adresi ve internetle iletişim kuran sistem ve nesnelerin oluşturduğu ağ olarak açıklanabilir. İkinci ise gerçek dünya içinde bulunan davranışların ve nesnelerin bilgisayar ortamı üzerinde bulunan simülasyon yardımıyla ortaya koyulan sanal ortam yapısıdır. Aynı zamanda siber fiziksel sistemler en az beceriye sahip insanların ve özel eğitimin olması gerektiği karışık vazifeleri en doğru ve en iyi şekilde yerine getirmesini sağlayan sistemler olarak da açıklanmaktadır. Böylece burada açıklanan sistemler çok daha verimli, zeki ve üretken bir şekilde olacaktır.

Sistemlerin fiziksel bileşenlerinin bağlantı kurdukları elemanlar vardır. Bu elemanlar arasında sürekli ve etkileşimli bir haberleşme kurmak için bulut yapısının bilişim teknolojisi ve interneti kullanmaktadırlar. Bu sayede verileri bir araya getirmek ve işleyerek uygun hale getirmek için bazı imkanlar sağlamaktadır. Bu imkanlar gerçek dünyayla mekânsal olarak ve gerçek zamanlı bir şekilde etkileşime girme olarak açıklanmaktadır.

Buradaki işlem birbirinden farklı haberleşme ağ yapılarında gerçekleşmektedir. Bunun yanı sıra ayrı katmanlarda bulunan ve ölçeği büyük yapılarda dinamik ve sürekli olarak çalışmaktadır. Tüm bu işlemler fiziksel bileşen adı verilen yapıya ve herhangi bir sisteme gömülü bir halde bulunan yazılım entegre sistemiyle oluşmaktadır. Siber fiziksel sistemlerle bileşenler ve makinelerin internet yapısıyla insanlarla ve diğer makinelerle haberleşme kurma becerisi fazlasıyla iyi olmaktadır.

Siber fiziksel sistem yapıları aynı zamanda algılama araçları, işlemciler, iletişim teknoloji sistemleri gibi donanımsal araçlar içinde bulunan yazılımlardan oluşur. Aynı zamanda bilgiyi doğal olarak değiştirebilen, yapılacak olayları başlatan ve birbirlerinden farklı olarak denetleyebilen sistemlerdir [5].



Şekil 1.1.1. Siber fiziksel sistemler [6]

Bu sistemler uyarlanabilirlik becerilerini yüksek seviyede otomasyon ve denetleme ile gerçekleştirmektedir. Aynı zamanda da yeniden yapılandırmaktadır. Bu da sistemin ve gerçekleştirecek olan işlemlerin güvenilirliğini en üst seviyede sağlamaktadır [7].

Siber fiziksel sistemlerle ilgili bileşen yapıları ve makinelerin internetle daha farklı diğer insan ve makinelerle iletişim ve bağlantı kurma becerisi bulunmaktadır. Siber fiziksel sistem yapıları aynı zamanda algılama araçları, işlemciler ve haberleşme teknoloji sistemleri gibi donanımsal araçların içinde yer alan yazılımlardan oluşmaktadır. Bunun yanında bilgiyi en doğal haliyle değiştiren, yapılan işlemleri başlatabilen ve birbirlerini bağımsız bir şekilde denetleyebilen sistemlerdir [5].

Siber fiziksel sistenler içinde yer alan siber çevre ise bilgisayar tabanlı cihazlarda çalışan yazılımı, bu cihazlarda depo edilen bilgiyi ya da cihazların ortaya çıkardığı bilgileri de içermektedir. Cihazların bulunduğu ortamlar ve servis yapılarını da siber çevrenin bir parçası şeklinde düşünülebilir. Siber ortam, sistemler üzerinde bulunan bütün yazılım uygulamalarını ve kullanıcı ağ yapılarını içinde bulundurmaktadır. Yine siber ortam içerisinde bulunan transit uygulama adı verilen uygulama yapıları ve depolama işlemleri dolaylı veya doğrudan ağlara bağlanabilmektedir. Böylece siber ortam, sistemlerin içerisinde bulunan bilgileri işleyen bir sistem olarak da açıklanmaktadır [8].

1.1.2. Siber Tehdit

Siber uzay adı verilen bir ortam vardır. Bu ortama özel olarak engelleyici, bozucu, yok edici ve tamamıyla ele geçirme gibi saldırı girişimleri yapılabilmektedir. Bu girişimlerle siber atakların farklı cihazlar ve metotlarla siber uzay adı verilen bu ortamda kullanılmasına siber tehdit adı verilmektedir. Buna ek olarak siber tehditler hem klasik suçların siber uzaya uygun hale getirilmiş durumlarına hem de haberleşme teknoloji sistemleri ve bilgilerden yararlanılarak ortaya çıkarılmış bütün yeni suç açıklamalarını da içine almaktadır [9].

Aynı zamanda siber tehditler bir bilgisayar ağı yapısına, bilgi teknolojisine, akli varlığa veya başka bir hassas veriye zarar verme olarak tanımlanmaktadır. Bununla birlikte siber tehditler, yetkisiz biçimde erişimde bulunmayı, bozmayı veya çalmayı hedefleyen başarılı olabilecek bir siber atak ihtimalini ortaya koymaktadır. Siber tehditler, güvenilir kullanıcılar tarafından bir kuruluş içinden veya bilinmeyen taraflarca uzak konumlardan gelebilir. Siber tehditlere sebep olan gruplara düşman devletler, terörist gruplar, kurumsal casuslar ve organize suç örgütleri, bilgisayar korsanları ve çok daha fazlası örnek verilebilir. Bu zararlı gruplar tarafından oluşturulan bazı siber tehdit türlerine ise kötü amaçlı yazılım, casus yazılım, kimlik avı saldırıları, dağıtılmış hizmet reddi (DDoS) saldırıları, sıfır gün istismarları ve buna benzer birçoğu daha örnek verilebilir. Son yıllarda yapılan siber tehditlere bakılacak olursak Covid temalı kimlik avı saldırıları, fidye yazılım saldırıları, tedarik zincir saldırıları ve e-dolandırıcılık en fazla yapılan siber tehditleri oluşturmaktadır [10].



Şekil 1.1.2. Siber tehditler ve bunların algılanması [11]

1.1.3. Siber Saldırı

Siber saldırı, siber ortam içerisinde bulunan bilgilerden yararlanmak, bu bilgileri ve oluşacak olan verileri bozmak, sistem yapılarının bağlanılmasını engellemek, bilgileri değiştirmek veya tüm bu ve bunun gibi kötü girişimlerle tüm sisteme zarar vermek hedefiyle siber ortamda yapılan işlemlerdir [12]. Siber saldırılar dünyanın her alanında en çok ihtiyaç duyulan bilgi sistemlerine zarar verir. Bu sistemlerin çalışmasını sağlayan bilgisayarlara zarar verir ve devre dışı bırakır. Her sektör yaptığı iş için kullandığı verileri çok büyük titizlikle ve güvenlikle saklamak ister. Siber saldırılar bu verilerin çalınmasına neden olur. Birbirinden farklı yöntemlerle bu saldırılar gerçekleştirilir [13].

Siber suçların yanı sıra siber ataklar bilgisayar korsanlarıyla özdeşleştirilebilir. Hatta siber terörizm veya siber savaş ile de özdeşleştirilebilir. Siber saldırılar iç tehditler ve dış tehditler olarak iki farklı şekilde algılanabilir. Hem içerden hem de dışarıdan yapılan siber saldırılar finansal verileri, çok önemli kişisel verileri, ticari sırlar ve fikri mülkiyetleri ve çok daha fazlasını elde etmek amacıyla yapılmaktadır. Yapılan bu siber saldırılar eğer amacına ulaşırsa sistem ve sunuculara, bir sistemde var olan verileri silebilir, değiştirebilir ve ekleyebilir, sistemde var olan değerleri bilgilerin elde edilmesine neden olabilir ve sistemi devre dışı bırakabilir. Örneğin bir fidye yazılımı çetesi olan DarkSide, 29 Nisan 2022'de ABD'nin rafine edilmiş büyük bir ürün hattı sistemi olan Colonial Pipeline'a saldırı. Sanal bir özel ağ (VPN) ve güvenliği ihlal edilmiş bir parola aracılığıyla u boru hattı siber saldırısı şirketin ağlarına girdi ve boru hattı operasyonlarını kesintiye uğrattı. Aslında DarkSide, ABD'nin doğu kıyısına tedarik edilen gaz, dizel ve jet yakıtının %45'ini taşıyan boru hattını kapattı. Kısa süre sonra, Colonial Pipeline CEO'sunun ödediği Bitcoin kripto para biriminde yaklaşık 5 milyon ABD doları talep eden bir fidye notu ile kapatmalarını izlediler [14].

Siber saldırılar günümüzde çok önemli bir yere sahiptir ve önümüzdeki yıllarda da en zor alanlardan birisi haline gelecektir. Sistem kullanıcılarını ve geliştiricilerini bu konuda bilgilendirmek ve eğitmek son derece önemli bir konudur. Siber dünya içinde bulunan kullanıcı kişilerin hem siber savunma becerilerini hem de siber saldırı becerilerini geliştirecek bilgiye sahip olmaları gerekmektedir. Ancak bunun sağlanması için çok sağlam bir algılama ve bilgi gerekliliğinin olması şarttır. Gerçekleştirilen bir atağın sonucu, seviyeli bir şekilde çok fazla etkilere neden olabilir. Günümüzde teknoloji ve teknolojinin oluşturduğu bütün sistemlere duyulan aşırı güven toplumdaki herkesi çok tehlikeli bir yola

sürükleyebilmektedir. Finansal şirketler, eğitim kurumları, sağlık hizmetleri, enerji hizmetleri, devlet hizmetleri ve çok daha fazlası yalnızca bir ağa bağlıdır. Bu bağlantı aynı zamanda küresel erişimli bir bağlantı olmaktadır. İnsanların ömürleri boyunca alacakları hizmetlerini güvende tutmak için her zaman siber ataklarla ilgili eğitimler yapılmalı ve toplum bu konuda bilinçli bir hale getirilmelidir [15].

Siber saldırıların toplam sayısı ve buna maruz kalan yapıların ekonomik olarak ne kadar zarar ettiğine dair kesin bilgilere ulaşmak imkansızdır. Bunun nedeni ise suçluların nadir olarak tespit edilmesi ve yetkili kurumlara bildirilmemesidir [16]. Bunun yanı sıra internet ortamı üzerinden yapılan saldırıları tespit etmek hiç kolay değildir [17]. Siber suçu işleyenlerin yakalanamamasının ve takibinin çok zor olmasının bazı nedenleri vardır. Belirlenemeyen postalar yani kimliği belli olmayan dosyaların, internet tarafından sağlanan üçüncü yapıdaki uygulamaların, şifrelemeye sahip cihazların, bilgisayara zarar vermek isteyen terör örgüt yapıları ve bilgisayar korsanlarıyla birlikte kullanılması bu sebeplerin en başlarındadır. Buna ek olarak bilişim suçlarının davalarının karışık bir yapıya sahiptir. Bu nedenle siber terörizm adı verilen olumsuz durumun kesin bir açıklaması ve ifadesi olmadığı için bu da davaların karışık olduğunu belirten nedenlerden olmaktadır [18,19,20].

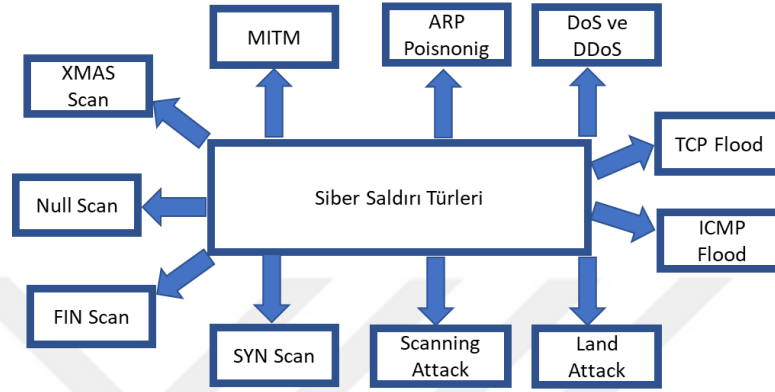
Amerika Birleşik Devletleri Ulusal Araştırma Konseyinde 2009 senesinde gerçekleştirilen bir çalışmada siber saldırılar farklı şekillerde tanımlanmaktadır. Bu tanımlardan birisi ise; “Ağlar, bilgisayar sistemleri veya bilgiyi ve bunlar içinde kalıcı olarak bulunan ya da bunları taşıyan programları bozmak, küçük düşürücü bir duruma getirmek, kandırmak ve ortadan kaldırmak için yapılan bilerek yani kasıtlı hareketler” tanımıdır [21].

1.1.4. Siber Saldırı Türleri

Şirketlerin veya sistemlerin güvenliğini ortadan kaldırmaya yönelik bilgilerin çalınması, casusluk ve maddi kazanç için yapılan kasıtlı ve iyi niyetli olmayan girişimler olarak adlandırılmaktadır. Bu saldırı türlerinin amacı geleneksel güvenlik çözümlerini, yapay zekâ ve analiz yöntemleriyle birlikte kullanılmaz bir hale getirmektir [22].

Siber saldırı türleri gene olarak üç aşamada değerlendirilebilir. Bunlardan birincisi finansal kazanç sağlamak, işleri kesintiye uğratmak amacıyla sistemleri hedef alan aktör ve

gruplardır. İkincisi politik nedenlerden dolayı bilgi toplamak. Üçüncüsü ise elektronik sistemleri panik ve korkuya uğratarak baltalamaya çalışmaktır [23].

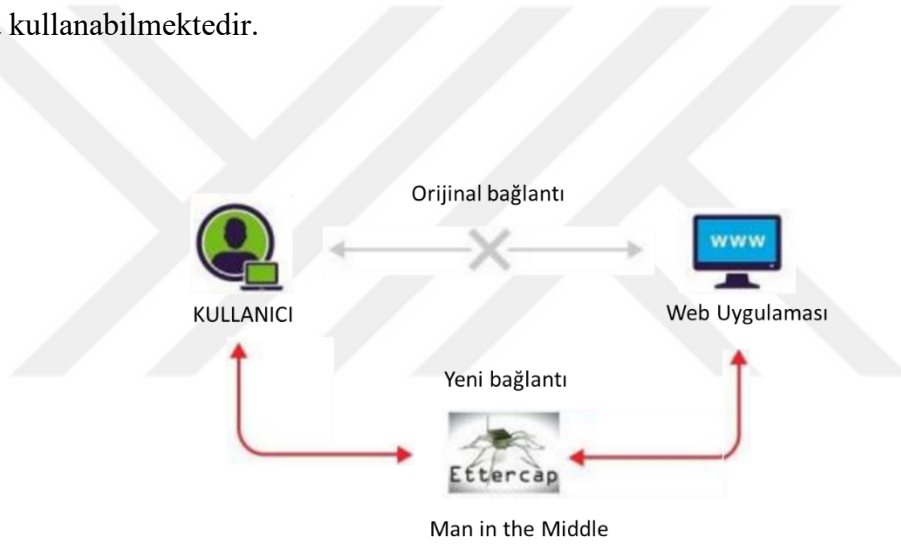


Şekil 1.1.4. Siber saldırı türleri genel görünümü

1.1.4.1. Man-In-The-Middle (MITM) Saldırısı

Ortakdaki adam saldırısı (MITM), kurban bilgisayarlar ve ağ cihazları arasında gerçekleşen bir saldırdır. Şifrelenmiş verileri takip ederek ve yetkisiz erişim sağlanarak verilerin gizlice yakalanması ve şifrelenen verilerin takip edilerek yapıldığı bir saldırı türüdür. Kullanıcıların bir organizasyon içinde bilgi paylaştığı iletişim kurduğu ilk yöntem ağ altyapı hizmetidir. Veri paketleri ağ içerisinde özgür bir şekilde gezinmektedir. Kendisinde bulunan IP adresinde olmayan bir paket yapısı alan araçlar isterlerse bu paketin içeriğini görebilir veya üzerinde değişiklik yapabilirler [24]. MITM saldırısı, ağdaki paketleri yakalamak ve bunları kendi faydasına kullanmak olarak da ifade edilebilir. Aynı zamanda ortakdaki adam saldırıları, iki yapı arasındaki haberleşmeyi kesintiye uğratması ve bir bilgisayar saldırganının önemli verileri hemen yakalamasına ve işlemesine izin vermesi nedeniyle çevrimiçi güvenlik açısından çok önemli bir tehdit oluşturmaktadır. Bu işlem gerçekleşirken saldırıya uğrayan kişi sanki herhangi bir saldırı meydana gelmemiş gibi internete bağlanarak bilgisayarını kullanmaya devam etmektedir. Buna rağmen bilgisayarla haberleşme kurulan tüm uygulamalar ve siteler görünür, açık hale gelmektedir. Burada

gerçekleştirilen bu saldırı, bütün konuşmaların saldırganlar tarafından denetlendiği bir tür gizli dinleme olarak da tanımlanmaktadır. Mesela, ana bilgisayar ve istemci arasında bir TCP bağlantısı bulunan HTTP işlemi olsun. Ayrı yöntemler uygulayan saldırgan, gerçek TCP bağlantısını yeni iki bağlantı şeklinde böler [25]. Birinci bağlantı saldırıya uğrayan kişi ile saldırgan arasındadır. İkinci bağlantı ise sunucu ve saldırgan arasında gerçekleşmektedir. TCP bağlantı yapısını saldırıyı yapan kişi keserek yakalanan iletişimdeki verileri okuyabilir veya üzerinde değişiklik yapabilmektedir. Buna ek olarak saldırgan kullanıcının tanımlama yaptığı bilgileri çalabilmektedir. Buradan alınan çerezler, bir kullanıcının oturumunu yakalamak ve saldırganın bu kullanıcıyı web sitesinde taklit etmesine olanak sağlamak amacıyla kullanabilmektedir.



Şekil 1.1.4.1. MITM saldırısı temsili görüntü. [26]

MITM saldırısı, aynı teknikleri kullanarak bunu bir https bağlantısı üzerinden de gerçekleştirebilir. Buradaki fark ise her TCP bağlantısı değil de yeni SSL oturumlarının kurulma durumudur. Burada farklı olan bu iki farklı bağlantıdan biri saldırgan ile tarayıcı arasında gerçekleştirilen SSL bağlantısı, diğeri ise web sunucu ile saldırgan arasındaki başka bir SSL bağlantısının gerçekleştirilmesidir. Bunun olduğu anlarda web tarayıcısı kullanıcıyı bu dijital sertifika kabul edilemez durumda olduğu bir alarm veya uyarı ile tetikler, fakat kullanıcı karışılacağı bu tehdidin farkında olmadığından dolayı alarmı yok sayar. SSL kullanılıyor olsa da saldırgan kullanıcıları SSLstrip ile http trafiğine yönlendirebilir. Tüm

trafiği izleyen saldırgan, girilen tüm siteleri gönderilen kullanıcı adı ve şifre bilgilerini net bir şekilde görebilmektedir. Saldırgan girilen tüm bilgileri Clear Text yapısı olarak da görebilmektedir. Sonuç olarak bir saldırgan kullanıcıların bilgilerinin neredeyse hepsini ele geçirebilir [24].

MITM saldırıları, aynı zamanda DNS sunucuları denilen yapıları da hedef olarak alabilmektedir. Alan adı sistemi yani DNS araması, web tarayıcı yapılarının alan adlarını IP adreslerine çeviren bir yapı olmaktadır. Daha sonrasında ise web sitelerini bulmayı sağlamaktadır. DNS sahtekarlığı, DNS ele geçirme ve DNS sahtekarlığı gibi ortadaki adam saldırılarında, saldırıyı yapan bir kişi DNS arama zamanı denilen bu zamanı tehlikeye atabilmektedir. Bununla birlikte kullanıcılar genellikle kötü amaçlı yazılım dağıtan veya hassas bilgiler toplayan siteleri doğru olmayan sitelere yönlendirebilir. Saldırgan daha sonra gerçek web sitesiyle arasında gerçekleştirilen yoğun trafiği takip etmek ve değiştirmek için bir Proxy yapısı gibi davranabilir. MITM saldırılarının daha yoğun bir şekilde yapıldığı alanlar çevrimiçi bankacılık ve e-ticaret web siteleridir. MITM yalnızca bir saldırı tekniği olarak düşünülmemelidir, bunun yansıra bir web uygulamasının geliştirme aşaması ve web güvenliğini sağlamak amacıyla, güvenliğin geliştirilmesi gereken yönlerini ortaya çıkaran bir yapıdır [26].

1.1.4.2. ARP Poisoning

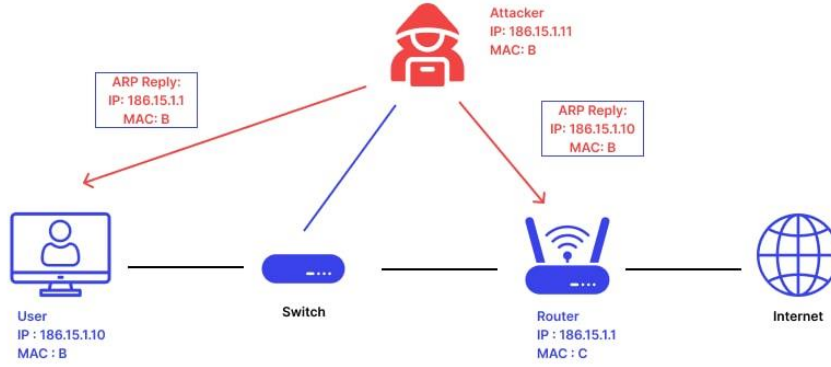
Adres Çözümleme Protokolü (ARP), bilgisayar ağları yapılarında gerçekleştirilen seviyeli veya katmanlı yaklaşıma destek olmak ve en iyi şekilde çalışmasını yerine getirmek amacıyla geçmişten bu yana her zaman var olmuştur. Buradaki katmanların her birinin bir görevi vardır. Bu görevler bazen bir Ethernet kablosu adı verilen materyal üzerinden giden elektrik sinyallerinden bir web sayfası meydana getirmek ve bazen de ilk HTML koduna kadar her zamanı gerçekleştirmektir. Bu katmanlar birbirinden bağımsız çalışmaktadırlar. Ağ katman teknolojisi olarak bilinen bluetooth ve IPv4 wifi gibi çok yeni teknolojilerle bir araya gelerek kullanılabilir. Bu haliyle kullanılması için veri bağlantı katman yapıları ve alt fiziksel yapılar, radyo dalgaları gibi belirli bir çevre üzerinden veri gönderimi yapması gerekmektedir.

ARP denilen bu yapının amacı, veri bağlantı katmanındaki adreslerle (MAC adresleri) ağ katmanındaki tipik bir şekilde olan IP adresleri arasında çeviri işlemi gerçekleştirmektedir. Ağ yapısına bağlı araçların, anında hangi cihaz veya araca belirlenen bir IP adresi atandığını “sorgulamasına” izin vermektedir. Burada kullanılan cihazlar aynı zamanda gerçekleştirilen bu eşleme işlemini istenmeden ağın geri kalan tarafında duyurabilir. Verimlilik adına, cihazlar tipik olarak bu yanıtları önbelleğe alır. Daha sonra MAC-IP eşlemelerinin bir listesini oluşturur [27].

ARP Zehirlenmesi saldırısı (ARP Poisoning), bir yerel alan ağı (LAN) üzerinden gerçekleştirilen ve IP’indeki eşleşmeleri, medya erişim kontrolü (MAC) adresine değiştirmek için bir LAN üzerindeki varsayılan ağ geçidine kötü amaçlı ARP paketleri göndermeyi amaçlayan bir siber saldırı türüdür. ARP protokolü, internet protokolü (IP) adreslerini MAC adreslerine çevirir. ARP protokolünün tasarımı amacı güvenlik değil de verimlilik amacıyla olduğundan saldırganın hedef LAN içindeki bir makinenin kontrolüne sahip olduğu veya doğrudan ona bağlı olduğu sürece ARP zehirlenmesi saldırılarının gerçekleştirilmesi oldukça kolaydır.

Saldırı, bir saldırganın varsayılan ağ geçidine kendi ait olan MAC adresinin hedefinin IP adresiyle özdeşleştirilmesinin gerekli olduğunu bildiren doğru olmayan bir ARP cevap mesajı göndermesiyle oluşmaktadır. Varsayılan olarak ayarlanmış olan ağ geçidi bu mesajı aldığı anda ve üzerinde meydana gelen değişikliklerini ağda bulunan tüm cihazlara açtıktan sonra, hedefin ağda bulunan diğer herhangi bir cihaza olan trafiğinin tamamı saldırganın bilgisayarından dolaşır ve saldırganın onu kontrol etmesine veya değiştirmesine izin verir.

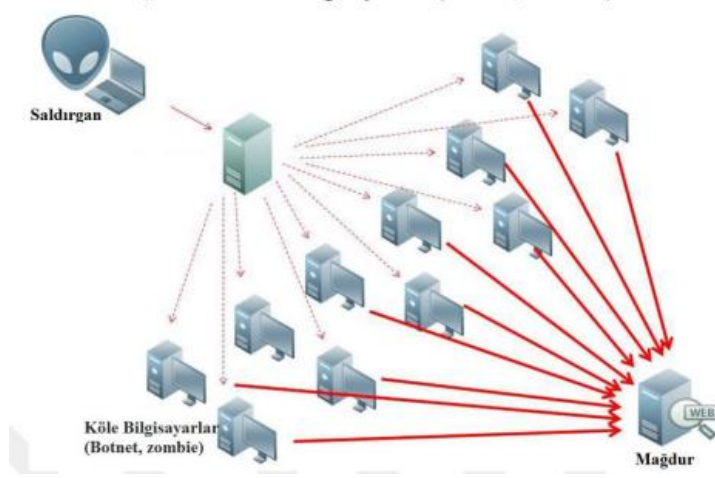
ARP zehirlenmesi saldırıları düşük bir seviyede gerçekleştiğinden, bu saldırı tarafından hedeflenen kullanıcılar, trafiklerinin denetlendiğini veya değiştirildiğini nadiren anlamaktadırlar. Ortadaki adam saldırılarının (Man In The Middle) yanı sıra, ARP zehirlenmesi, hedefin paketlerini iletmeden, yalnızca araya girerek veya düşürerek bir LAN üzerinden hizmet reddi durumuna neden olmaktadır [28].



Şekil 1.1.4.2. ARP zehirlenmesi saldırısı görüntüsü [29]

1.1.4.3. Dos ve DDoS Saldırıları

Öncelikli olarak sunucu olan herhangi bir bilgisayara eş zamanlı ve aynı zamanda mümkün oldukça çok paket gönderilmektedir. Buradaki amaç burada kullanılan bilgisayar kullanıcılarının hizmet veremez ve iş göremez hale gelmesini sağlamaktır. Bu duruma hizmet reddi saldırısı (Denial Of Service Attack- DoS) denir. Bunun yanı sıra bu saldırılar güvenlik zafiyetlerinden ve açıklarında faydalanabilirler. Bunun sonucunda da zorlu yollarla alınmış ve kullanıcıların bilgisi dışında uzaktan yönetilebilen köle bilgisayarların (zombi, bot) kullanılmasıyla yapılan dağıtık hizmet reddi saldırısı (Distributed Denial Of Service Attack- DDoS) adı verilen saldırı oluşmaktadır. DDoS saldırılarının kuvveti ve etkinliği, DoS saldırıların kuvvetinden köle bilgisayar araçlarının sayısı ile çarpılması ölçüsünde fazla olacağı için çağımızda çok daha sıklıkla kullanılır olmaktadır. DDoS saldırısı bağlı olduğu bir sistem yapısının ve bir hedef bilgisayarın saniyeler içerisinde binlerce belki de on binlerce bilgisayarın atağına maruz kalarak kullanılamamasına neden olacak kadar etkilidir [9].



Şekil 1.1.4.3. Köle bilgisayarların (Zombi, Botnet) görünümü [30]

DoS saldırısı esnasında bir bilgisayar saldırıya maruz kalan kullanıcının bilgisayarına büyük miktarda trafik gönderir ve onu kapatır. DoS saldırısı, bir web sitesinde yapıldığında web sitesini kullanıcılar için kullanılamaz hale getirmek için yapılan çevrimiçi bir saldırı olmaktadır. Bu saldırıyı internete çok sayıda trafik göndererek internete bağlı web sunucusuna yapmaktadır [30].

DDoS saldırısı yapılırken bir sunucu hedef olarak alınır. Daha sonra bu sunucunun hizmeti veya ağın normal trafiği, hedefi ve çevresinde bulunan altyapıyı bir internet trafiği akışıyla ezerek bozmaya yönelik kötü niyetli bir girişim olarak tanımlanmaktadır. Bu saldırılar güvenliği ihlal edilmiş birden çok bilgisayar sistemini saldırı trafiği kaynağı olarak kullanarak etkili olmaktadır. Bu saldırılar internete bağlı araçların ağları ile gerçekleştirilir [31].

DoS ve DDoS saldırılarının türleri vardır. Bu saldırılardan bazıları gözyaşı saldırısı (Teardrop Attack), IP parçalama saldırısı (IP Fragmentation Attack), protokol saldırısı (Protocol Attack), uygulama tabanlı saldırı (Application Based Attack) ve Hacimsel Saldırı (Volumetric Attack) [32].

DoS ve DDoS saldırıları arasında bazı farklar vardır. Bu farklar ise aşağıda verilen tabloda görülmektedir [30].

Tablo 1.1.4.3. DoS ve DDoS saldırılarının karşılaştırılması

Hizmet Reddi Saldırısı (DoS)	Dağıtık Hizmet Reddi Saldırısı (DDoS)
Tek bir sistem kurbanın sistemine saldırır.	Birden fazla sistem kurbanın sistemine saldırır.
Kurban bilgisayarı tek bir konumdan gelen veri paketiyle yüklenir.	Kurban bilgisayarı çoklu konumdan gelen veri paketiyle yüklenir.
DDoS saldırısına göre daha yavaştır.	DoS saldırısına göre daha hızlıdır.
Tek sistem kullanıldığı için kolayca bloke edilebilir.	Birden fazla cihaz paket gönderip birden fazla yerden saldırıldığı için bu saldırıyı engellemek zordur.
Saldırıları izlemek kolaydır.	Saldırıları izlemek zordur.
Trafik hacmi DDoS'a göre daha azdır.	Trafik hacmi DoS'a göre daha fazladır.

1.1.4.4. TCP Flood

İletim kontrol protokolü (Transmission Control Protocol – TCP), bilgisayarlar arasındaki haberleşmenin, küçük paketler şeklinde ve kayıp olmadan gerçekleştirilmesine öncülük eden bir protokoldür. Bu protokolün sağladığı en önemli özellik veriyi alıcıya gönderirken veya alırken kimlik doğrulaması yaparak veri bütünlüğünü sağlamasıdır [33].

TCP seli saldırıları, TCP senkronize (synchronize – SYN) seli saldırılar veya SYN seli saldırıları olarak da adlandırılmaktadır [34].

TCP protokolü kullanılarak istemci ve sunucu arasında bir oturum başlatıldığında, oturumu oluşturan ‘üçlü el sıkışması’ iletilerine sunucu belleğinde küçük bir arabellek alanı ayrılır. Oturumu başlatan paketler, ileti alışverişindeki diziyi tanımlayan bir SYN alanı içerir. SYN seli saldırıları ise bu süreci bozmayı amaçlamaktadır. Bir saldırgan çok sayıda bağlantı isteğini hızlı bir şekilde gönderir ve sunucu tarafında her paket için küçük bir alan ayrılmaya başlanır. Ardından gelen paket sayısındaki fazlalık limitlerin dolmasına ve sunucunun yanıt veremez hale gelmesine neden olur. Bu saldırı, saldırganın bir bağlantı istemesi, ancak bağlantı dizisinin geri kalanını hiçbir zaman tamamlamaması şeklinde de ifade edilebilir. SYN seli saldırıları, mevcut sunucu kaynaklarını tüketerek trafiğe kapatmayı amaçlayan önemli bir DDoS saldırısıdır.

SYN seli saldırıları bir TCP bağlantısının üçlü el sıkışma sürecini kötü niyetli olarak kullanır. TCP bağlantı iletişimi üçlü el sıkışma ve güvenli bağlantıyı amaçlamaktadır. Normal koşullar altında, TCP bağlantısı herhangi bir bağlantı kurmak için bazı işlemler

göstermektedir. İlk olarak, istemci bağlantıyı başlatmak için sunucuya bir SYN (senkronize et) mesajı gönderir. İkinci olarak sunucu daha sonra iletişimi onaylamak için bu ilk pakete bir SYN/ACK (eşzamanlama- onaylama) mesajı ile yanıt verir. Daha sonra mesajın sunucudan alındığını onaylamak için bir ACK mesajı döndürür. Bu mesaj gönderme ve alma sıralaması tamamlandıktan sonra, TCP bağlantısı açılır ve veri gönderilip alınır.

Siber saldırgan, hizmet reddi oluşturmak için, ilk SYN mesajının alınmasının ardından sunucu yapısının bir veya daha çok SYN/ACK mesajla cevap vermesini ve el sıkışma işleminin son adımının gerçekleşmesini beklemeyiz. Bu anda sunucu da bir hafıza alanı bağlantı süresi dolana tek kilitlenir.



Şekil 1.1.4.4. TCP flood saldırısı görüntüsü [34]

SYN seli saldırısının işleyişi şu adımlarla ifade edilebilir.

- Saldırgan, hedeflenen sunucuya genellikle sahte IP adresleriyle çok yüksek hacimde SYN mesajları gönderir.
- Daha sonra sunucu bağlantı isteklerinin her birine yanıt verir ve yanıt almaya hazır bir açık bağlantı noktası bırakır.
- Sunucu hiçbir zaman ulaşmayan son ACK mesajını beklerken, saldırgan daha fazla SYN mesajı göndermeye devam eder.
- Her yeni SYN mesajını gelişi, sunucunun belirli bir süre için yeniden açık bir bağlantı noktasını geçici olarak sürdürmesine ve bütün kullanılabilir bağlantı

noktaları tüketildikten sonra sunucu kilitlenmeye ve hizmet verememeye başlar.

Bir SYN seli saldırısı birkaç farklı şekilde meydana gelebilir. Saldırı şekilleri doğrudan saldırı, sahte saldırı ve dağıtılmış saldırılar olarak ifade edilmektedir [35].

1.1.4.5. ICMP Flood

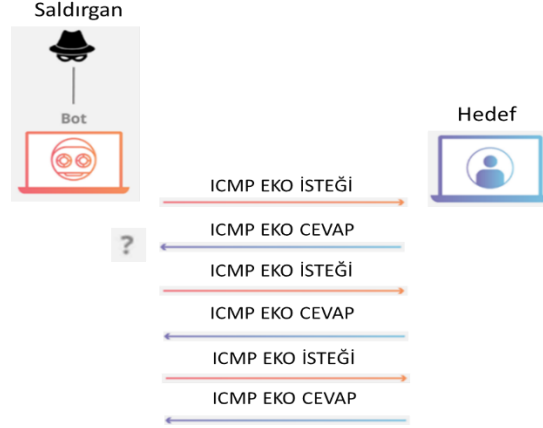
İnternet kontrol mesaj protokolü (Internet Control Message Protocol – ICMP), ağ cihazlarına ve ana bilgisayarlarla kontrol mesajları göndermek için kullanılmaktadır [36].

ICMP yapısının bazı görevleri vardır. Bu görevlerden bazıları internet protokolünün (IP) kontrol edilmesi olabileceği veya hata bildirimini yapması için kullanılan bir alt protokolde olabilmektedir. Bu yapı aynı zamanda hem bir yönlendirici ve ana bilgisayarların bulunmadığını belirten hata mesajlarının oluşturulması ve gönderilmesi hem de belirli bir hizmetin var olup olmadığını belirten bir yapı olarak da tanımlanmaktadır [37].

ICMP seli saldırısı, ping seli (Ping Flood) saldırısı olarak da tanımlanmaktadır. Saldırısı yapan bir kişinin kurban bilgisayarını ping adı verilen ICMP yankı istekleriyle ederek aldığı yaygın ve çok geniş bir hizmet reddi (DoS) saldırısıdır.

Normalde, ping istekleri, bir ICMP yankı isteği gönderildiğinden bir ICMP yankı yanıtı alındığında gidiş dönüş süresini ölçerek iki bilgisayarın bağlantısını test etmek için kullanılır. Ancak bir saldırı sırasında, hedef paketleri ile veri ağı aşırı yüklenmek için kullanılır. Bir ping seli yürütmek, saldırganın hedeflerinin IP adreslerini son derece iyi bir şekilde bilmesine bağlıdır. Bu nedenle saldırılar hedefe ve IP adresinin nasıl çözüldüğüne bağlı olmaktadır. Buda üç farklı şekilde incelenebilmektedir.

Bunlardan birincisi hedeflenen bir yerel ifşa (A targeted local disclosed), ikincisi bir yönlendirici (A router disclosed) ve üçüncüsü kör bir ping (A blind ping flood) şeklindedir.



Şekil 1.1.4.5. ICMP flood saldırı görüntüsü [39]

Hedeflenen bir yerel ifşa edilen ping seli saldırısı yerel bir ağdaki tek bir bilgisayarı hedefler. Saldırının IP adresini bulması için bilgisayara fiziksel olarak erişmesi gerekmektedir. Başarılı bir saldırı, hedefteki bilgisayarın kapatılmasına neden olmaktadır.

Bir yönlendirici seli saldırısı, bir ağdaki bilgisayarlar arasındaki iletişimi kesmek için yönlendiricileri hedef almaktadır. Bu saldırıda saldırının yerel bir yönlendiricinin dahili IP adresini bilmesi gerekmektedir. Başarılı bir saldırı, yönlendiriciye bağlı tüm bilgisayarların kapatılmasına neden olmaktadır.

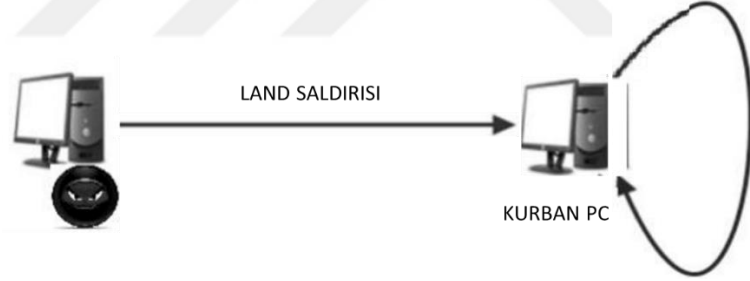
Kör bir ping seli saldırısı, bir saldırının yapılmadan önce yönlendiricinin veya hedef bilgisayarın yönlendiricinin IP adresini meydana çıkarmak için dışarıdan bir program kullanmayı hedeflemektedir [38].

1.1.4.6. Land Attack

Bir yerel alan ağı reddi (LAND attack) saldırısı, herhangi bir bilgisayara sahte paketler göndererek bilgisayarların kilitlemesine neden olan bir saldırıdır. Bu saldırının gerçekleştirildiği açık tarihte ilk olarak 1997 yılında ‘m3lt’ takma adını kullanan biri tarafından keşfedilmiştir. Yıllar sonra Windows Server 2003 ve Windows XP SP2 gibi işletim sistemlerinde yeniden ortaya çıkmıştır [40].

Land saldırısı, saldırganın bir TCP segmentinin kaynak ve hedef bilgilerini aynı olacak şekilde ayarladığı bir hizmet reddi saldırısı (DoS) saldırısıdır. Güvenlik açığına sahip olan bir makine, paketin TCP tarafından tekrar tekrar işlenmesinden dolayı çökecek veya donacaktır.

Bir LAND saldırısında, bağlantı noktası ve kaynak IP adresi, bağlantı noktası ve hedef adresle aynı olacak ve bu da kurbanın makinesinde açık bir bağlantı noktasına işaret edecek şekilde ayarlanacak özel bir şekilde hazırlanmış bir TCP SYN paketi oluşturur. Güvenlik açığı bulunan herhangi bir makine, böyle bir mesajı alır ve paketi yeniden işlemek için sonsuz bir döngü şeklinde gönderir ve hedef adrese yanıt verir. Bu sebeple, makine CPU'su savunması zayıf olan makinenin donmasına, kilitlenmesine ve hatta çökmesine neden olmaktadır. Bu saldırı açıklarının [40]'da bahsedilen örneklerine ek olarak klasik CISCO IOS yazılımı ve HP Jetdirect Baskı Sunucularının da bu tür saldırılara karşı savunmasız olduğunu bildiren CERT danışma belgesi yayınlanmıştır [41].



Şekil 1.1.4.6. Land saldırısı temsili görüntü [42]

Şekil 1.1.4.6' da görüldüğü üzere saldırganlar aynı kaynak ve hedef adrese sahip olacak şekilde kötü niyetli paketler göndermektedir. Hem ana bilgisayar hem de kaynak adresleri kurban adresleridir. Çoğunlukla yerel alan ağlarında kullanılır. Kurban sistem bu paketleri aldıktan sonra kilitlenir ve kendisine yanıt verir. Sistem buradaki saldırıyı algılayana kadar ve kapatana kadar bu döngü devam etmektedir [42].

1.1.4.7. Scanning Attack

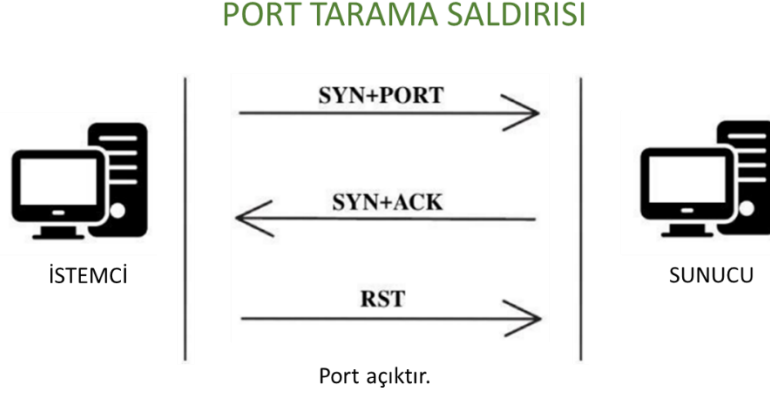
Etik korsanlıkta tarama bir kuruluşun ağına bağlı sistemleri tanımlamak için kullanılan bir ağ araştırma tekniğidir. Hedef sistemdeki erişilebilir sistemler, kaynaklar ve hizmetler hakkında bilgi sağlamaktadır. Bazı kesimler bu taramayı etkin tarama olarak adlandırmaktadır. Çünkü bu duyarlı olan ana bilgisayarlarda hizmetleri kesintiye uğratabilir. Tarama, genellikle mevcut savunmalardaki zayıflıkları araştırmaktadır. Aynı zamanda da güvenlik açığı değerlendirmesi sırasında kullanılmaktadır.

Tarama, hedef sistemdeki açık bağlantı noktalarını belirlemeye ve bağlantı noktası eşlemesi yapmaktadır. Bu bağlantı noktaları aracılığıyla işletim sistemiyle etkileşimli bir oturum gerçekleştirme veya hatta bu açık bağlantı noktalarından gelen trafiği yeniden yönlendirmek için kullanılabilir. Bir tarama sayesinde gerçekleştirilebilecek birçok görev vardır.

Tarama ağ içerisinde bulunan tüm etkin adresleri taramak için IP adresleri ve ağ maskeleri listesi oluşturmak kadar kolay bir işlem olabilmektedir. Buna ping taraması denir. Diğer başka bir yöntem ise TCP SYN paketlerini hedef sistemdeki yanıt bekleyen bağlantı noktalarına gönderen ve aynı zamanda etkin bir tarama olan bir bağlantı noktası taramasıdır. SYN bağlantı noktası taraması, açık olan ve yanıt bekleyen bağlantı noktalarına TCP SYN paketleri ve bir bağlantı noktasının kapalı olduğu anlamına gelen (RST/ACK) bir RST paketi gönderir.

Tarama tekniklerinin türleri TCP bağlantı taraması ve TCP SYN port taraması olarak adlandırılabilir [43].

Saldırganlar, sistemleri zarara uğrattırırken birçok taktik, teknik ve prosedür (Tactic, Technical, Procedure – TTP) üretmektedir. Bu TTP'ler PRE-ATT&CK ve ATT&CK [44,45]'de anlatılmaktadır. Bunlardan birincisini saldırganlar hedef hakkında bilgi toplamak için kullanırken, ikincisini ise bu hedeften yararlanmak için kullanmaktadırlar. Tarama saldırısı PRE ATT&CK' da bilgi toplamak için kullanılan teknik yöntemlerden birisidir. Saldırganlar tarama saldırısını yaptıktan sonra toplanan bu bilgiler doğrultusunda sistemlere girmeyi amaçlamaktadır.



Şekil 1.1.4.7. Scanning attack görüntüsü [48]

[46]'da olduğu gibi birçok saldırıdan önce tarama saldırıları kullanılmaktadır. Temel olarak üç tür tarama saldırısı vardır. Bunlar yatay bağlantı tarama noktası saldırısı, dikey bağlantı noktası tarama saldırısı ve ana bilgisayar tarama saldırısıdır. Yatay bağlantı tarama noktası saldırısı, TCP veya kullanıcı datagram protokolü (User Datagram Protocol – UDP) paketlerini bir hedef ana bilgisayarın birden çok bağlantı noktasına göndererek kullanılabilir bağlantı noktalarını arar. Dikey bağlantı noktası tarama saldırısı, ağdaki birden çok hedef ana bilgisayarın bağlantı noktasına TCP ve UDP paketleri göndererek belirli bir bağlantı noktası açan ana bilgisayarları aramaktadır. Bir ana bilgisayar tarama saldırısı, ping gibi komutları kullanarak ağdaki birden çok ana bilgisayara ICMP yankı istekleri göndererek iletişim kuran ana bilgisayarları aramaktadır [47].

Tarama saldırıları için Nmap tarayıcısı çok önemlidir. Bilgisayar ağları alanında uzman olarak bilinen Gordon Lyon (Fyodor) tarafından geliştirilerek ortaya çıkmış bir güvenlik tarayıcısı yapısıdır. Ağın haritasını tarayarak çıkarmaktadır. Aynı zamanda makinelerde çalışan servis yapılarının durumlarını, portların durumlarını ve işletim sistemlerini gözlemleyebilmektedir. Nmap'ın kullanım alanları oldukça geniştir. Bu alanlar, taranan ağdaki sistemlerle ilgili bilgi sahibi olunması (portta çalışan uygulama vb. bilgileri kavramak ve öğrenmek için), ağ topolojisi yapısının çıkarılması, sızma testlerinin gerçekleştirilmesi, bir ağ ayarlanırken gerekli olan testlerin yapılması, ağ envanterinin kaydedilmesi, bakımı, haritalanması ve yönetimidir.

```

C:\>nmap -T5 -sV -O orgaring.org
Starting Nmap 4.76 ( http://nmap.org ) at 2009-03-19 12:01 GTB Standart Saati
Interesting ports on rr.remedy.orgaring.org (208.115.12.12)
Not shown: 997 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 4.7p1 Debian Subuntu1.2 (protocol 2.0)
80/tcp    open  http         Apache httpd
179/tcp   open  tcpwrapped
Device type: WAP|general purpose|broadband router|media device|firewall
Running (OST GUESSING): Linksys embedded (91%), Linux 2.4.X/2.6.X (91%), Roku embedded (90%), 3Com Linux 2.4.X (89%), Aladdin Linux 2.4.X (89%), FON Linux 2.6.X/2.4.X (89%), Siemens embedded (88%)
Aggressive OS guesses: Linksys WAP54G WAP (91%), Linux 2.4.32 (x86) (91%), Linksys WRV54G wireless broadband router (90%), Linux 2.6.13 - 2.6.24 (90%), Linux 2.6.17 - 2.6.22 (90%), Linux 2.4.18 - 2.4.32 (likely embedded) (90%), Linux 2.4.9 - 2.4.18 (likely embedded) (90%), Linux 2.6.17 - 2.6.25 (90%), Linux 2.6.9 - 2.6.26 (90%), Roku HD1500 media player (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 14 hops
Service Info: OS: Linux
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.23 seconds
C:\>

```

Şekil 1.1.4.8. Nmap çalışma zamanı görüntüsü [49]

Nmap bir sunucu veya istemciyi birçok ayrı biçimde tarama becerisine sahiptir. Nmap yapısını güçlü yapan özelliği tarama metotlarına sahip olmasından gelmektedir. Protokol yapılı (UDP, TCP, vb.) tarama yapabilmektedir. Aynı zamanda bazı belirlenen aralıklardaki IP adresleri, alt ağ yapıları (subnet) ve üzerlerinde çalışan servis ve port işlevleri de taranabilmektedir [50,51].

Nmap tarama türleri vardır. Bu türler ise FIN Scan, TCP SYN Scan, Null Scan, XMAS Scan ve daha fazlasıdır. Aşağıda burada belirtilen türlere kısaca değinelim.

1.1.4.7.1. SYN Scan

Kaynak olarak bulunan makinenin hedef tarafında olan makineye TCP SYN bayraklı bir şekilde bir segment göndermesiyle başlayan bir tarama saldırısı çeşididir. Portların kapalı bir şekilde bulunduğu durumlarda hedef olarak yer alan makine yanıt olarak RST ACK bayrak yapılı bir segment döndürür. Portların açık olduğu durumlarda ise hedef makine SYN ACK bayraklı segment döndürmektedir. Daha sonra kaynak tarafında bulunan makine RST bayraklı segment yapısını göndererek kurulmuş olan bağlantıyı kesmektedir. Böylelikle TCP üçlü el sıkışma tamamlanmamış olur. Bu tarama türünde TCP üçlü el sıkışma adı verilen olay gerçekleşmediğinden dolayı bu tarama çeşidi hedef sisteminde bir iz bırakmaz [50].

1.1.4.7.2. FIN Scan

Hedef tarafında bulunan makineye TCP bağlantı isteği yapılmadan iletilen segmentle tarama yapılmaktadır. Kaynak olan makinenin ileteceği FIN bayraklı segment yapısı, hedef olan makinenin kapalı şekilde bulunan bir portuna gelebilir. Bu durumda hedef olan makine RST ACK bayraklı segment yapısını döndürmektedir. Eğer açık bir şekilde olan portuna gelirse hedef olan makineden bir cevap geri gelmeyecektir [50].

1.1.4.7.3. Null Scan

Hiçbir bayrak yapısını barındırmayan bu tarama saldırı çeşidi, gerçek yaşamda karşılaşılmayan türdür. Kaynak olan makinenin ileteceği bayraksız segment yapıları karşısında hedef tarafta yer alan makinenin vereceği cevaplar FIN Scan ile aynı olmaktadır. Kaynak tarafındaki makinenin ileteceği bayraksız segment yapısı, hedef olan makinenin kapalı bir portuna geldiği takdirde hedef tarafında yer alan makine RST ACK bayraklı segment yapısını döndürmektedir. Eğer port açık olursa hedef makineden herhangi bir tepki dönmeyecektir [50].

1.1.4.7.4. XMAS Scan

Bu tarama saldırısında ise kaynak tarafta bulunan bilgisayarın TCP segment yapısına URG (belirli verilerin acil olduğunu belirtir), PSH (uygulama katmanında hemen verileri itme) ve FIN (bağlantıyı kapatır) bayrak yapılarını atayacağı ('1' olacağı) segment olarak bulunan hedef tarafındaki makineye gönderilir. Eğer kaynak tarafta bulunan makinenin ileteceği FIN, URG ve PSH bayraklı segment yapıları, hedef olarak bulunan makinenin kapalı bir portuna gelebilmektedir. Bu şekilde olursa hedef olan makine RST ACK bayraklı segment yapısını iletecektir. Port eğer açık bir durumda olursa hedef tarafında yer alan makineden bir cevap dönüşü olmayacaktır.

Burada açıklanan tarama türüne TCP başlık yapısı içinde bulunan altı tane bayrak yapısından yalnızca üç tanesi ('1' yapıldığı) ayarlanmaktadır. Bundan dolayı gönderilen

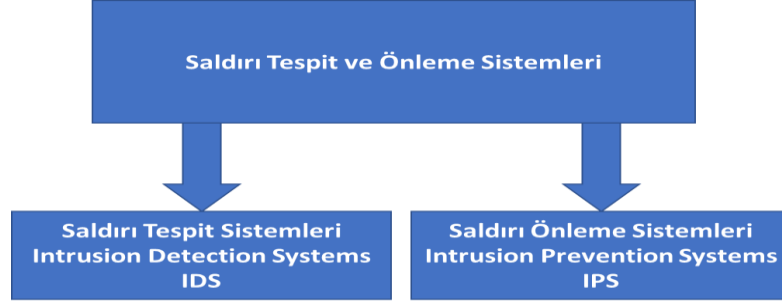
segment yapısı yılbaşında görülen süslenmiş ağaçlarda bulunan lambalara benzetilmiştir. Bu sebeple bu tarama çeşidine de XMAS (Christmas) Scan adı verilmektedir [50].

1.1.5. Saldırı Tespit ve Önleme Sistemleri

Günümüzde internet ağları karışık ve anlaşılması zor bir yapıya sahiptir. Bundan dolayı, siber saldırıların zaman geçtikçe daha farklı türleri ortaya çıkmaktadır. Bunun yanında saldırılar hızlı bir şekilde artmaktadır. Ağ sistemlerinde görülen bu karışıklık geleneksel olarak ortaya konulan şifreleme ve güvenlik duvarı yapıları ile korunamamaktadır. Ortaya çıkan bu zorluktan dolayı sistemlerin içerisinde bulunan ağ trafiğinin sürekli olarak izlenmesi gerekmektedir. Yapılan izleme ile saldırı girişimlerinin gerçek zamanlı olarak tespit edilmesi gerekmektedir. Muhtemel bir saldırı, ihlal ve tehditlerin tespitinin yapılması için ağ üzerinde gerçekleşen aksiyonların ve trafiğin analiz edilmesi gerekmektedir. Tüm bu yöntemleri kapsayan yapı ise saldırı tespit sistemleridir. Bu yönüyle saldırı tespit sistemleri çok önemli bir güvenlik aracı haline gelmiştir.

Saldırı önleme sistemleri ise, saldırıların tespit edilip önlenmesi işlemlerini sağlayan ağ güvenlik sistemlerini oluşturmaktadır. Saldırı tespit sistemleri (Intrusion Detection Systems – IDS) ve saldırı önleme sistemleri (Intrusion Prevention Systems), ağı çok sık bir şekilde gözlemlemektedir. Bununla birlikte oluşabilecek olan tehditleri tanımlamaları gerekmektedir. Dahası oluşacak olan durumların kayıtları tutması gerekmektedir. Tanımlamak ve kayıtları tutmak görevi dışında saldırıları durdurmak ve güvenlikten sorumlu yetkililere rapor vermek gibi çok önemli görevleri yerine getirmektedir.

Bu sistemler bazı anlarda şirket ve kurumların güvenlik politikalarında oluşabilecek her türlü savunmasız durumu ve zafiyeti meydana çıkarmak için de kullanılabilir. Aynı zamanda saldırı engelleme sistemleri saldırganların ağlarla ilgili bilgi toplama faaliyetlerini algılar ve saldırganların sistemle ilgili bilgi almasını engellemektedir. Aynı zamanda bu anda durdurma işlemi de gerçekleştirilebilir [52].



Şekil 1.1.5. Saldırı tespit ve önleme sistemleri genel sınıflandırma

Saldırı tespit sistemleri ve saldırı önleme sistemleri, siber ortam savunmasının ilk hattıdır. Bu sistemler, ihlalleri ve saldırıları yakalamak için geliştirilmiştir. Bir IPS ve IDS sisteminden kaçmak siber güvenlikte büyük bir boşluğun yaratılmasına neden olur [53].

Saldırı tespit sistemleri ve saldırı önleme sistemleri ağ güvenliği için çok önemli sistemlerdir. Bilgisayar ağlarındaki gerçekçi dağıtım ve yapılandırma yoluyla güvenlik politikalarını ihlal eden eylemleri tespit etmek için yetkisiz girişler ve anormal durumlar tespit edilebilir ve raporlanabilir. Bu sistemler arasındaki iş birliği çok üst düzeyde olmaktadır [54].

1.1.5.1. Saldırı Tespit Sistemleri

Saldırı tespit sistemi (Intrusion Detection System -IDS), bir ağı izleyen bir cihaz veya yazılım uygulamasıdır. Bu izleme işlemini ise politika ihlalleri ve kötü amaçlı etkinliklerden dolayı yapmaktadır. Sistemlere karşı yapılan kötü amaçlı bir etkinlik veya güvenlik ihlali durumlarını yönetim sistemi yapısı kullanılarak raporlanır ve kaydedilmektedir [55].

Saldırı tespit sisteminde anormallik algılama ve raporlama birinci asıl görev olsa da bazı izinsiz giriş algılama sistemleri, bazı şüpheli IP adreslerinden gönderilen trafiğin engellenmesi de dahil olmak üzere, kötü amaçlı etkinlik ve anormal trafik algılandığında eylemde bulunabilir. Bir IDS, IDS ağ paketlerini potansiyel olarak zarar veren ağ trafiğine karşı izleyen, ancak ilk amacı tehditleri tespit etmek ve kaydetmek yerine, tespit edildikten

sonra tehditleri önlemek olan saldırı önleme sistemi (Intrusion Prevention System- IPS) ile karıştırılabilir.

Saldırı tespit sistemleri bilgisayar korsanlarının gerçek bir ağa zarar vermeden önce yakalamak için ve anormal olan durumları tespit etmek için kullanılmaktadır. IDS'ler ağ veya ana bilgisayar tabanlı olabilmektedirler. Ana bilgisayar tabanlı olacak şekilde istemci bir bilgisayara saldırı tespit sistemi kurulmaktadır. Böylece ağda ağ tabanlı bir şekilde kullanılan saldırı tespit sistemi yer almaktadır. Saldırı tespit sistemleri, bilinen saldırıların imzalarını arayarak veya normal olmayan durumları arayarak çalışmaktadır. Bu sapmalar ve normal olmayan durumlar oluşturulan yığında yukarıya doğru itilir. Daha sonra bu durumlar protokol ve uygulama katmanında incelenir. Bir saldırı tespit sistemi, müşterilerin donanımsal yapıları üzerinde çalışan bir yazılım uygulaması olabileceği gibi bir ağ güvenlik aracıda olabilmektedir [56].



Şekil 1.1.5.1. Saldırı tespit sistemi çalışma görüntüsü [57]

Saldırı tespit sistemleri beş farklı tipe ayrılmaktadır [58];

- Ağ saldırı tespit sistemi (Network Intrusion Detection System – NIDS)
- Host saldırı tespit sistemi (Host Intrusion Detection System – HIDS)
- Protokol tabanlı saldırı tespit sistemi (Protocol-Based Intrusion Detection System – PIDS)

- Uygulama protokolü tabanlı saldırı tespit sistemi (Application Protocol-Based Intrusion Detection System – APIDS)
- Hibrit saldırı tespit sistemi (Hybrid Intrusion Detection System – HIDS)

Saldırı tespit sistemleri saldırıyı tespit etmede imza tabanlı tespit (Signature-based detection-SD), anormallik tabanlı tespit (Anomaly-based Detection-AD) ve durum bilgi protokol analizi (Stateful Protocol Analysis – SPA) olmak üzere iç farklı şekilde sınıflandırılmaktadır. İmza tabanlı tespit sisteminde imza bilinen bir saldırı veya tehdide karşılık gelen bir kalıptır. İmza tabanlı tespit sistemi olası izinsiz girişleri tanımak için imzaları yakalanan olaylarla karşılaştırmaktadır. Anormallik tabanlı tespit sisteminde anormallik bilinen bir davranıştan sapmaktır. Bu tespit sisteminde ise önemli saldırıları tanımak için normal profilleri gözlemlenen olaylarla karşılaştırılarak tespit yapılır. Durum bilgi protokol analizi ise belirli protokollere yönelik genel profillere bakarak tespit yapan bir tespit sistemidir [59].

1.1.5.2. Saldırı Önleme Sistemleri

Saldırı önleme sistemi (Intrusion Prevention System – IPS), belirli bir ağı kötü amaçlı etkinliklere karşı sürekli olarak izleyen ve saldırı gerçekleştiğinde bunu raporlama, engelleme veya bırakma dahil olmak üzere bunları önlemek için harekete geçen bir ağ güvenlik aracıdır. Bu araç bir donanım aygıtı veya bir yazılım uygulaması olabilmektedir. Bir saldırı veya ihlal olduğunda bunları basitçe algılamanın ve bu kötü amaçlı girişimleri ilgili yöneticilere bildirmekle kalmamaktadır. Bu saldırı ve ihlallere karşı önlem alamayan saldırı tespit sistemlerinden bu yönüyle ayrılmaktadır [60].

Saldırı önleme sistemi, tanımlanmış tehditleri tespit etmek ve önlemek amacıyla çalışan bir ağ güvenliği olarak da tanımlanmaktadır. Saldırı önleme sistemleri, ağları sürekli izleyerek, olası kötü amaçlı olayları arar ve bu olaylar hakkında bilgi toplamaktadır. Saldırı önleme sistemleri bu olayları sistem yöneticisine bildirir. Bu sayede erişim noktalarının kapatılması ve güvenlik duvarlarının gelecekteki saldırıları önlemesi adına sistemin yapılandırılması gibi önleyici eylemler alınmış olmaktadır. Saldırı önleme sistemleri ayrıca, kurumsal güvenlik politikalarındaki sorunları belirlemek, çalışanları ve ağa misafir

olarak giren kullanıcıları bu politikalardan bulunan kuralları ihlal etmekten caydırmak için de kullanılabilir [61].



Şekil 1.1.5.2. Saldırı önleme sistemi örnek görüntü [62]

Saldırı önleme sistemi, yönlendirilen ağ trafiğini tarayarak çalışmaktadır. Bu tarama işlemini ise yapılan ihlaller, alışılmamış saldırı yapıları ve kötü niyetli faaliyetler için aktif bir şekilde tarayarak yapmaktadır. IPS motoru adı verilen yapı ağ trafiğinin hepsini analiz etmektedir. Daha sonra ise bilinen saldırı kalıpları için bit akışı denilen dahili imza veri tabanı ile aralıksız bir şekilde karşılaştırma yapmaktadır. Bir IPS, kötü niyetli olduğu bilinen bir paketi bırakabilir ve bu işi, saldırıyı gerçekleştiren kişinin adresinden ve bağlantı noktasından gelecek tüm trafiği engeller. Aynı zamanda da takip eder. Kötü niyetli olmayan normal bir trafik ise herhangi bir kesinti olmaksızın çalışmaya devam edebilir. Saldırı önleme sistemleri, trafik paketlerini izlemek ve bunlara yanıt vermek gibi daha karmaşık gözlem ve analizlerde yapabilmektedir [63]. Bu algılama mekanizmaları ise aşağıda yer alan tabloda yer alan yapıları içerebilir.

Tablo 1.1.5.2. IPS yapısının algılama mekanizmaları

Saldırı Önleme Sistemleri(Intrusion Prevention System - IPS)
Adres değiştirme
http dizesi ve alt dize eşleştirmesi
Genel desen eşleştirme
TCP bağlantı analizi
Paket anormalliği algılama
Trafik anormalliği algılama
TCP/UDP bağlantı noktası eşleşmesi

Bir saldırı önleme sistemi, tipik olarak gözlemlediği olaylarla ilgili tüm bilgileri kayıt altına alır. Bu kayıtların sonucunda güvenlik yöneticilerini bilgilendirir ve raporlar üretir. Bir ağın güvenliğini sağlamaya yardımcı olmak için bir IPS, ortaya çıkan internet tehditlerini sürekli olarak izlemek ve engellemek için önleme ve güvenlik güncellemelerini otomatik olarak alabilmektedir [63].

Saldırı önleme sisteminin birçok faydası vardır. Şekil 1.1.5.3'te de olduğu gibi bu faydaların bazılarını görebiliriz.



Şekil 1.1.5.3. Saldırı önleme sistemleri genel görüntüsü [64]

1.1.6. Mevcut Çalışmalar

Sayegh ve arkadaşlarının ortaya koydukları çalışmalarda [79] önceki dönemlerde SCADA sistemine karşı gerçekleştirilen saldırılardan ve bu saldırıların ortaya çıkardığı çok önemli sonuçlardan bahsedilmiştir. Ortaya çıkan bu olayların kaydedilen verileri endüstriyel sistemler açısından güvenlik örnekleri isimli veritabanında yayımlanmaktadır [80]. OMRON bir üretici şirkettir. Bu üreticinin, üretmiş olduğu cihazlar kullanılarak test ortamı oluşturulmuştur. Bu ortam içerisinde bulunan her araç ve gereç Ethernet bağlantısıyla dağıtıcı adı verilen bir cihazla haberleşmektedir. Aynı zamanda PLC, saha cihazı ve HMI olarak kullanılmaktadır. Bunun sonucunda ise üreticiye ait seri haberleşme protokolüyle haberleşme gerçekleştirilmektedir. Oluşturulan test ortamında bazı saldırılar gerçekleştirilmiştir. Bu saldırılar ise yeniden göndermek saldırısı (replay), kriptolojik ataklar ve DoS saldırısıdır.

Zhu ve arkadaşlarının ortaya koydukları çalışmada [81] SCADA sisteminin geleneksel olarak tanımlanan bilgi teknolojilerinden ayrılan tarafları ve SCADA sistemini koruma altına almak için mevcut tehlikeler ayrıntılı bir şekilde incelenmiş ve analiz edilmiştir. SCADA sistemi direkt olarak fiziksel dünyayla ilişkilidir. Bunun dolayı sistemden elde edilen sonuçlar doğa ve insan hayatı üzerinde doğrudan izlenmektedir. Ayrıca SCADA sisteminin düşük gecikmeli çalışma gereksinimi, zaman kritik çalışma gereksinimi ve geniş çevre etkisi gibi sistemsel zorlukları vardır. SCADA sisteminde oluşacak küçük bir zaman gecikmesi bütün saha ve çevredeki işlerin zamanının gecikmesine ve sağlanacak hizmetin kesintiye uğramasını sağlayacaktır. Burada dile getirilen nedenlerden dolayı basit yapıdaki protokoller ve gerçek zamanlı işletim sistemlerinin birlikte kullanılmasıyla sistem minimum oranda kullanılmaktadır. SCADA sisteminin karakteristik özelliği vardır. Bu özelliğinden dolayı bilgi iletişim teknolojilerine oranla farklılık göstermektedir. Bilgi iletişim teknolojileri güvenliği ve gizliliği temel alan tasarımlardan meydana gelmektedir. Ancak SCADA sistemi sürekli hiç durmadan çalışma mantığı ve zaman kritikliği yapısı temel alınarak tasarlanmıştır. SCADA sistemi donanım, yazılım ve iletişim açısından çok sayıda saldırıya uğramaktadır.

Davidson ve arkadaşlarının yaptığı çalışmada [82] SCADA sisteminin araç ve gereçleri temel alınarak yapılan genel atak vektörleri ve savunma mekanizmalarının analiz edilmesi üzerinde çalışılmıştır. Sahada bulunan teçhizatların uzaktan kontrolünün

sağlanabilmesi ve yönetilmesi için haberleşme ortamlarını kullanmaktadır. Bunu yaparken kontrol merkezine ulaşmaları gerekmektedir. Kontrol merkezi ve saha ekipmanlarının iletişimi esnasında bazı teknikler kullanılmaktadır. Bu teknikler ise şifreleme ve güçlü kimlik doğrulamadır. Kimlik doğrulama ve şifreleme ve tekniklerinin olmadığı bir durumda paketlere müdahale etmeyi sağlamaktadır. Paket değişikliğinin temel alınarak yapıldığı saldırılarda sahada istenmeyen değişiklikler görülebilir. Denetleme merkezinin aldığı paketlerde yapılabilecek değişiklikler, sahanın gözlemlenmesi esnasında sağlanan verilerin yanlış verilerle değiş tokuş edilmesine sebep olacaktır. Böylece denetleme merkezi tüm ortamı istendiği şekilde kontrol edemeyecektir. Buna ek olarak sahadan alınan verilerin gerçekliğinden de şüphe duyulacaktır. Kontrol ve verilerin gözlemlenmesi için kullanılan veri paketinin boyutu küçüktür. Bu nedenle ağ kapasiteleri sınırlıdır. Sınırlı olan ağ kapasitesi servis dışı bırakma atağı yapılmasıyla birlikte haberleşme ağ yapısının çökmesi ve saha ile iletişimin durdurulmasına neden olacaktır. Bu durum çok tehlikeli ve kötü durumlar meydana getirebilir. Bunun yanı sıra yapılan fiziksel ataklarla PLC mekanizmasında çalışan kod yapısında da değişiklikler yapılması mümkündür.

Leverett ve arkadaşlarının ortaya koydukları çalışmada [83] endüstriyel kontrol sistemleri yapısının internete bağlanma durumunun çevrimiçi olarak saldırılara maruz kalmasına neden olmaktadır. Yapılan bu saldırıların hedefi çoğu zaman zarar verme, sosyal mesaj ve sabotaj amaçlıdır. Tehditlere karşılık olarak alınan savunma için regülasyon yapıları ortaya koyulmaktadır. Regülasyon yapılarında bulunan bağlantı zamanlarının tersine endüstriyel kontrol sistemleri çoğu zaman internet bağlantısını aktif olarak her zaman kullanmaktadır. Haberleşme açık olarak paylaşılmamaktadır. Bu da sistemin keşfedilemez olduğu düşüncesini ortaya koymaktadır. Bunun sonucunda da sistemlerin güvenli olduğu düşüncesi hâkim olmaktadır. Yapılan çalışmada endüstriyel kontrol sistemleri arama motoru kullanımı ile analiz edilmiştir. Yapılan analizin sonucunda ise 7500 cihazın keşfedilebilir olduğu ortaya koyulmaktadır.

Krotofil ve arkadaşlarının ortaya koydukları çalışmada [84] sahada yer alan çevresel olarak elde edilen verilerin ölçümünü yapan sensörlere karşı tehlikelerden ve güvenlik açıklarından bahsedilmiştir. Sahada gerçekleştirilen işlemleri gerçekçi ve doğru bir şekilde yürütebilmesi için en önemli şey sahadan gelen doğru ve net veridir. Verilerin doğru ve gerçekçi bir şekilde gelebilmesi için sensörlerin güvenliği çok önemli bir konudur. Sensör araçlarının güvenliği en iyi şekilde sağlamak adına fiziksel ataklardan uzak durmak ve

kaçınmak çok önemlidir. Alınan verilerin gerçekliği ve doğruluğu için bazı yöntemler önerilmektedir. Bu yöntemler fiziksel kimlik doğrulama yöntemleri olarak tanıtılmaktadır.

Djouadi ve arkadaşlarının ortaya koydukları çalışmada [85] sahada bulunan araçlara ve ekipmanlara karşı gerçekleştirilen sonlu enerji saldırısı ve sınırlandırma saldırısıyla ilgili çalışılmıştır. Sonlu enerji saldırısı motifikasyon adı verilen işi ve kaybı, dürtü saldırı yapıları ve sonlu zaman saldırı yapıları gibi saldırılara karşılık gelmektedir. Sınırlandırma saldırısı potansiyel bir biçimde uzun saldırı olayları ve senaryoları sınıfını içine almaktadır. Servis dışı bırakma saldırısı, denetleme sinyali iptal etmekten oluşmaktadır. Böylece bu saldırı sınıflarının özel bir şeklini ortaya koymaktadır.

Mitchell ve arkadaşlarının ortaya koydukları çalışmada [86] hesaplama kaynakları adı verilen yapılara karşı yapılan solucan saldırısı, virüs saldırısı ve servis dışı bırakma saldırıları gibi saldırılar incelenmektedir. Denetleme sistemlerine ölçümlerde yapılan hatalar veya bazı tutarsızlıkların olması durumunda doğru olmayan yani hatalı uyarılar oluşturulmaktadır. Oluşturulan bu alarmin gerçek olumsuz ve riskli bir durumu işaret etmesi gerekmektedir. Bundan dolayı tespit sistemleri oluşmuş olan durumları anlayarak gerçek uyarılar ortaya koyması gerekmektedir. Bunun yanı sıra saldırganın haberleşme için kullanılan şifreleme anahtarını alması veya ağa bağlı olan araçlara müdahalede bulunabilmesi kritik bir durumdur. Bu durum bütünlük ilkesine karşı yapılan bir atak çeşidi olduğuna değinilmiştir.

Morris ve Gao'nun ortaya koydukları çalışmada [87] MODBUS protokol yapısına karşı yapılan saldırıları ve açıklıkları önlemeye yönelik çözüm önerileri sunmaktadır. Modbus protokol yapısı fonksiyon kodlarıyla çalışmaktadır. Aynı zamanda da herkese açık bir şekilde çalışmaktadır. Adres taraması işlemiyse fonksiyon kodları kullanılarak yapılmaktadır. Böylece cihazların keşfi yapılmıştır. Keşfi yapılan bütün cihazlarda diğer fonksiyon kodlarının incelenmesi yapılmaktadır. Yapılan bu inceleme sonucunda sistem içinde bulunan komut setleri yapısı ve cihazlar ortaya koyulmuştur. Bütün araçların tanımlaması yapılarak sistem içindeki cihazların çalışma durumları, üreticiye ait isimler ve versiyon numaraları gibi bilgiler alınmaktadır. Alınan bu bilgiler daha sonra değerlendirilmektedir. Bu değerlendirme sonucunda sisteme veya cihaza özel açıklık ve zafiyet durumları ortaya çıkarılmıştır. Ortaya koyulan sonuçlarla DoS saldırısının denemesi yapılmıştır. Modbus paketi içerisinde döngüsel artıklık kontrolü (Cycle Redundancy Check-CRC) kodlama verisi bulunmaktadır. Bu kodlama verisi bilinçli bir şekilde yanlış girilmiştir. Böylece CRC paketi uyumsuz olmuştur. Bu uyumsuzluk durumu bozuk paket durumunun

olduğu anlamına gelmektedir. Aynı zamanda burada alıcı paketi sanki görmemiş gibi davranmasına neden olmaktadır. Ancak denetleme esnasında geçen zaman ve paketlerin yoğun olma durumları sistemin işleyiş mekanizmasını oldukça kesintiye uğratmaktadır. Belirli sayıdaki paket sayısından sonra sistem yapısı diğer araçlardan gelen normal paket yapılarını alamamaktadır. Buna ek olarak sistem cevap veremez bir duruma gelmektedir.

Bhatia ve arkadaşlarının ortaya koydukları çalışmada [88] sahada bulunan elemanlar yani araçlar ve denetleme merkezi arasında bulunan haberleşme ağına bir atak yapılmıştır. Bu atak servis dışı bırakma saldırısıdır. Sahada bulunan araçlar ve denetleme merkezi arasındaki ağ paket yapıları kaydediciler içinde bulunan küçük ebatlı verilerle çalışmaktadır. Bundan dolayı ağ paket yapılarının ebatı bilgi işlem teknoloji sistemlerine oranla epeyce küçük olmaktadır. Güvenlik protokollerindeki güvenlik mekanizması yapısının olmaması sahada faaliyet gösteren araçlarda kimlik doğrulama işlemini gerçekleştirememektedir. İletilen emir saha aracında doğrudan çalıştırılmaktadır. Yapılan bu akademik çalışmada saha aracının gönderen denetlemesi yapmamasından yararlanılarak atak senaryosu ortaya koyulmuştur. Burada sözü edilen senaryo denetleme merkezi tarafından gönderilen geçerli emir saha aracında işlenmeden hemen önce saldırgan tarafından emir iletilmektedir. Böylece yeni gelen geçerli olmayan komut, geçerli komutun üzerine yazılmak durumunda kalmıştır.

Das ve arkadaşlarının ortaya koyduğu çalışmada [89] hata tespit sistemini (Intrusion Detection System – IDS) tanımlamakta ve ağ saldırı tespit sistemi (Network Intrusion Detection System- NIDS) tasarımında kullanılan önde gelen makine öğrenmesi (Machine Learning – ML) ve derin öğrenme (Deep Learning- DL) yöntemlerine dayalı olarak geliştirilen taksonomiye detaylı bir şekilde açıklamaktadır. Çeşitli seçeneklerin yararlarını ve zayıflıklarını ana hatlarıyla belirtmek için NIDS tabanlı makalelerin ayrıntılı bir şekilde analizi tartışılmaktadır. ML ve DL dahil olmak üzere yeni teknoloji ve NIDS teknolojilerindeki gelişmeler, metodoloji, değerlendirme ölçütleri ve veri seti seçimleri açıklanmaktadır. Makine öğrenimi ve derin öğrenme tabanlı NIDS'i geliştirmek için NIDS çalışmasının uzun vadeli kapsamıyla mevcut araştırma zorlukları vurgulanarak saldırı tespit sistemi ile başa çıkmak için birçok yeni teknik kullanılmaktadır. Ancak tehditlerin yüzeyi farklı cihazların arayüzleri ile katlanarak büyüdüğü için çoğu siber güvenlik savunma sistemlerinin dinamik ve karmaşık doğasına uyum sağlamak için yeterince hızlı olmamaktadır. Bu çalışma aynı zamanda derin öğrenme tekniklerini kullanan çeşitli saldırı tespit sistemi yetenekleri ve varlıklarının bir incelenmesini önermektedir. Ayrıca yanlış

alarm oranını otomatik olarak azaltmak ve algılama süreçleri zamanını optimize etmek için siber savunma mimarisinin ağ saldırı tespitini otomatik uygulamak adına fikirler önermektedir.

Ahn ve arkadaşlarının çalışmasında [90] bal küpü saldırı yöntemlerinden biri olan adres çözünürlük protokolü yanıltma saldırısı ile birleştirilen gelişmiş bir denetleyici kontrol ve veri toplama ağ mimarisi geliştirilmiştir. Bu mimarinin denetleyici kontrol ve veri toplama sistemi güvenliği konusunda daha iyi performans sağlayacağı öne sürülmüştür.

Jagtap ve arkadaşları çalışmasında [104] süreç kontrol ağ paketlerinde gerçekleşen izinsiz girişlerin tespiti yapılmaktadır. Bu çalışmada gas- pipeline veri seti kullanılmıştır.

Shitharth ve arkadaşları çalışmasında [105] SCADA sistemine karşı yapılan izinsiz girişlerin tespiti yapılmaktadır. Bu çalışmada ADFA-LD veri seti kullanılmıştır.

Jiang ve arkadaşları çalışmasında [106] veri akışlarına karşı yapılan kötü niyetli veri girişimlerini tespit etmek amacıyla yapılmaktadır. Bu çalışmada Transmission & distribution veri setleri kullanılmıştır.

Simon ve arkadaşlarının çalışmasında [107] endüstriyel operasyon içeren ağ verilerine karşı yapılan saldırıların keşfi yapılmaktadır. Bu çalışmada 2 Public veri seti kullanılmıştır.

Philips ve arkadaşlarının çalışmasında [108] SCADA sistemlerine ve Modbus protokolüne karşı yeni güvenlik tehditlerinin tespiti yapılmaktadır. Bu çalışmada Public veri seti kullanılmıştır.

Rosa ve arkadaşlarının çalışmasında [109] SCADA sistemlerine karşı yapılan anomali tespiti yapılmaktadır. Bu çalışmada gas-pipeline veri seti kullanılmaktadır.

Muhammed ve arkadaşlarının çalışmasında [110] birçok endüstri sistemine karşı yapılan saldırıların tespiti yapılmaktadır. Bu çalışmada (KDD)-Cap99 veri seti kullanılmaktadır.

Tahir Emre'nin çalışmasında [111] bir web sitesinin kimlik hırsızlığı olup olmadığını tahmin etmek amacıyla yapılmıştır. Bu çalışmada website phishing veri seti kullanılmıştır.

Faramondi ve arkadaşlarının çalışmasında [112] SCADA sistemine karşı yapılan hataların tespiti yapılmaktadır. Bu çalışmada WDT veri seti kullanılmıştır.

1.1.7. Denetim Kontrolü ve Veri Toplama Sistemi

Denetim kontrolü ve veri toplama sistemi (Supervisory Control and Data Acquisition – SCADA), ekipmanları ve koşulları kontrol etmek için uzak konumlardan gerçek zamanlı olarak veri toplama ve endüstriyel süreçleri kontrol etmeye yönelik bir yazılım uygulaması olarak adlandırılmaktadır. SCADA, endüstriyel süreçleriyle ilgili kuruluşlara verilere dayalı kararlar almak ve uygulamak için gereken araçları sağlamaktadır. En yaygın kullanılan endüstriyel kontrol sistemi türlerinden biri olan SCADA, neredeyse her tür endüstriyel süreci kontrol etmek için kullanılabilmektedir. SCADA hem donanım hem de yazılım bileşenleri içermektedir. Donanım bileşenleri verileri toplar, işler ve zamanında diğer sistemlere iletir. SCADA sistemleri, ayrıca sürecin durumunu ve sorunlarını raporlamak için tüm olayları kaydeder. SCADA sistemleri koşullar tehlikeli bir hale geldiğinde alarmlar üretmektedir [65].

Endüstriyel süreçler çok dikkatli bir koordinasyon ve hassasiyet gerektirmektedir. Bu SCADA sistemleri, gerçek zamanlı veri toplamak, verimliliği en üst düzeye çıkarmak, genel giderleri azaltmak ve operasyonları kolaylaştırmak gibi işlevler sağlamaktadır. Birçok endüstriyel kuruluş, denetim kontrolü ve veri toplama sistemine güvenmektedir. Operatörlerin verilere erişmesine ve ekipmanları yönetmesine imkân tanımaktadır. SCADA sistemi, endüstriyel ekipmanlardan veri toplamak, analiz etmek ve görselleştirmek için tasarlanmış güçlü bir kontrol sistemidir. Bu sistemler sıcaklık, titreşim, güç kullanımı gibi çok önemli ölçümleri görüntüleyebilmektedir. Modern SCADA sisteminin en önemli özelliklerinden birisi de operatörlere ve saha denetçilerine, her saha cihazını fiziksel olarak ziyaret etmeden verilere erişme, dönüştürme ve yönetme gibi olanaklar sağlamasıdır. Bunun sonucunda maliyet olarak çok önemli bir tasarruf sağlanmış olmaktadır [66].



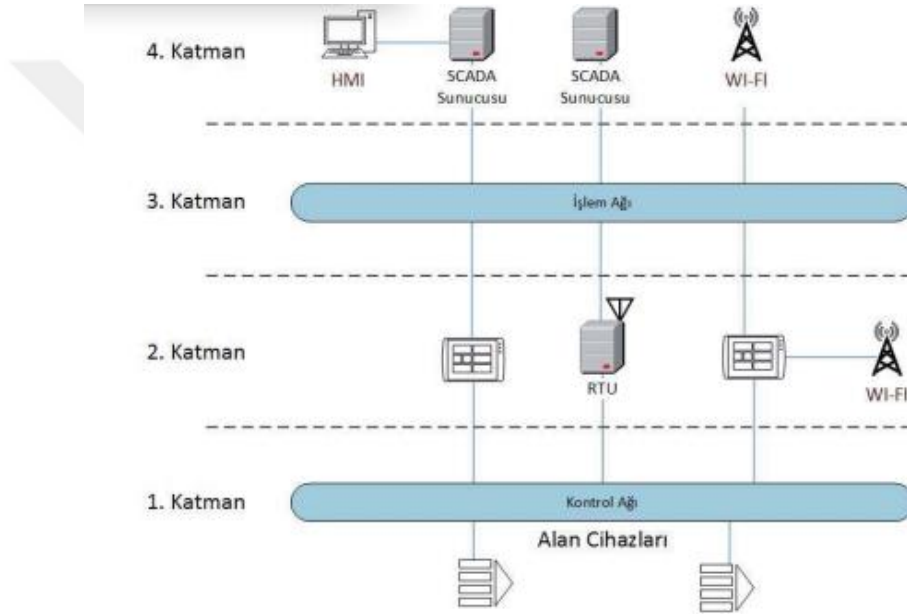
Şekil 1.1.7. SCADA yazılım uygulama örnek görüntüsü [67]

SCADA yazılım uygulamaları, endüstriyel sistemlerde altyapı yazılım görevini üstlenmektedir. Bununla birlikte fabrika içindeki ve dış yapısında bulunan ağlara bağlantı gerçekleştirerek şirketlerin bütün seviyelerinin ahenk içinde çalışma gerçekleştirmesine olanak sağlamaktadır. Böylece SCADA işletmelere çoğu zaman erişim sağlayabilecekleri ayrıntılı bir bilgi ve gerçek zamanlı doğru bir bilgi sağlama imkânı sunmaktadır [68].

1.1.7.1. Denetim Kontrolü ve Veri Toplama Sisteminin Yapısı

SCADA sistemi dört ana katman yapısından oluşmaktadır. Bu katmanlardan en altta bulunan katman sistemin dünya ile fiziksel olarak haberleşmesini sağlamaktadır. Bu haberleşme sağlanırken sürücüler kullanılmaktadır. Sürücü ve sensörler sayesinde fiziksel olaylar gerçekleştirilmektedir. Aynı zamanda sürücü ve sensörler sayesinde gerçekleştirilen fiziksel olaylar izlenebilmektedir. Burada anlatılan sensörün gerçekleştirdiği saha metrikleri sıcaklık, basınç ve devir gibi fiziksel verileri ortaya koymaktadır. Bu verilerin sistem tarafından anlaşılabilmesi gerekmektedir. Bu nedenle gerçekleştirilen fiziksel değişimler yine sürücü ve sensörler sayesinde analog ve dijital veriye dönüştürülmektedir. Algılanmak istenen bu sensör araçları fiziksel değişimin türüne göre değişim göstermektedir. Aynı veri tipleri, farklı türdeki sensör araçlarından alınan verileri tutmaktadır. Sahada ölçümü yapılan

verilerin değerlendirilmesi gerekmektedir. Bu değerlendirme sonucunda ortaya çıkan sonuçlarla sahadaki fiziksel bir olayı tetiklemek gerekebilir. Bu amaçla sürücü aygıtları kullanılmaktadır. Sürücü aygıtları çevre içinde bulunan vana, motor ve anahtar gibi elektrik ile çalışan metriklere iletilen gücün ve kuvvetin denetlenebilmesi amacıyla kullanılan bir devre aracıdır. Bu seviyede yer alan devre araçlarının işlem gücü bulunmamaktadır. Bu nedenle üst seviyeden alınan denetim sinyaliyle işlemler gerçekleştirilmektedir [70].



Şekil 1.1.7.1. SCADA katman yapısı ile temsil edilmesi [69]

Kontrol sisteminin aktarıldığı ortam kontrol ağı olarak tanımlanmaktadır. Kontrol ağında oluşturulan yapı devre elemanının üst katmanda yer alan cihazla arasındaki bağlantı uzaklığına göre değişkenlik gösterebilmektedir. Genellikle bu yapılar yakın bir şekilde konumlandırılabilen devre elemanları ve saha cihazları seri haberleşme kullanmaktadır.

Üst katmanda yer alan bilgisayar sistemleri ile alt katmanda bulunan devre elemanları protokoller ile haberleşme sağlamaktadır. Hesaplama yetkinliği, farklı protokollerin kullanılmasından dolayı farklı yetkinlikteki cihazların birbirleriyle iletişimi bu katmanda gerçekleşmektedir. Bilgisayar sistemi tarafından belirlenen protokolle iletilen komut ve emir

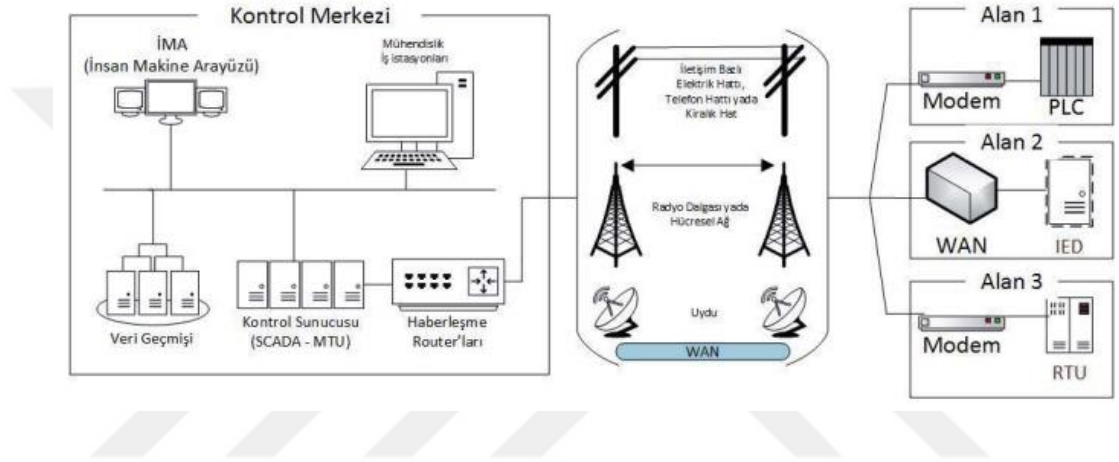
bu seviyede denetim sinyaline dönüştürülmesi gerçekleştirilmektedir. Sonrasında denetim ağı vasıtasıyla devre aracına gönderilmesi sağlanmaktadır. Bu seviyede yer alan araçların protokol yorumlama yetkinlikleri ve farklı ortamları destekleyen modülleri sayesinde gelen komutlar farklılık gösterse de aynı denetleme sinyalini oluşturmaktadırlar. Böylece kontrol katmanı içerisinde bulunan cihaz ayrılıkları, zaman süreci ağındaki iletişim ortamı ve protokol ayrılıkları sisteme herhangi bir etkisi olmamaktadır.

Katmanda bazı yapılar bulunmaktadır. Bu yapılar ise genel olarak uzak terminal birimi (Remote Terminal Unit- RTU) ve programlanabilir lojik kontrol (Programmable Logic Controllers- PLC) gibi saha cihazları olmaktadır. RTU, sahada yer alan analog ve dijital parametreleri okumaktadır. Daha sonra ise bu verileri merkezi izleme birimine aktarmaktadır. Sahada gerekli olan işlemlerin yapılması gerekmektedir. Bu nedenle birbirinden farklı bölümlerden meydana gelen devre kartı aygıtına sahip olmaktadır. Ufak yapıli denetleme sistemlerinde BASIC adı verilen programlama dili kullanılmaktadır. Büyük ölçekli denetleme sistemlerindeyse kablosuz haberleşme yapı ve mekanizmalarıyla faaliyet göstermektedir. Böylece oldukça büyük boyuta sahip sahalardan veri toplama işlemi yapılmaktadır.

[70]' de açıklandığı gibi PLC, sıcaklık, toz, titreşim gibi oldukça çetin koşullara karşı dayanıklı bir şekilde üretilmiştir. Kontrol sistemlerine göre şekillendirilmiş sınırlı hesaplama gücüne sahiptir. Endüstriyel amaçlarla kullanılan programlanabilir bir cihazdır. Bilgisayar sistemlerinin henüz gelişmiş olmadığı zamanlarda röle ve zamanlayıcı gibi bileşenlerin birbiriyle bağlantısı yapılarak kullanılmaktaydı. Yüzlerce ekipmanı bir araya toplamakla uğraşmak yerine farklı bir çözüm sunulmuştur. Bu çözüm ise PLC cihazlarının kullanılmaya başlanmasıdır. PLC programlanmasında ladder logic (merdiven lojiği) denilen yapı kullanılmıştır. Bu yapılar C ve röleler ile oluşturulmuş bir şematik diyagram şeklindedir.

Saha cihazlarıyla veriler anlamlı bir hale gelmiştir. Bu anlamlı verilerin kurulum anında meydana getirilen yapıya uygun bir şekilde denetleme merkezine iletilmesi için süreç ağı katmanı bulunmaktadır. Süreç ağı denilen yapı fiziksel çevre etkenlerine bağlıdır. Bu bağıllıkla iletişim çevrelerini ve protokollerini kullanarak saha araçları ve bilgisayar sistemiyle haberleşmeyi sağlamaktadır. SCADA sistemleri bilgisayar ağı yapılarıyla birlikte çalışmaya başlamıştır. Bununla birlikte süreç ağında geniş ağı ve yerel ağı yapıları kullanılmaya başlanmıştır. İletişim ortamı uzaklığa ve kullanılmakta olan ağı yapısına göre değişiklik göstermektedir. Kapalı çevrelerde faaliyet gösteren yapılarda genel olarak kablolu

iletişim kullanılmaktadır. Bu şekilde de bir yerel ağ oluşturulmuş olmaktadır. SCADA sistemleri geniş bir sahada görünmektedir. Bu şekilde de geniş alan ağı yapıları kurulmaktadır ve kullanılmaktadır. Aynı zamandan kablosuz çözümlerde kullanılmaktadır. Bu çözümlerin kullanılması ise operasyon sahasının büyüklüğüne göre şekillenmektedir. GSM, Wi-Fi ve uydu iletişimleri kullanılan kablosuz çözümler arasındadır [70].



Şekil 1.1.7.2. Modern SCADA sistemi [70]

[70]'de bahsedildiği üzere süreç ağı katmanında kullanılan protokoller kontrol merkezinde yer alan yazılıma ve kullanılan saha cihazlarına bağlı olarak değişiklik göstermektedir. Üreticiler geleneksel iletişim protokollerini kullanmaktadır. Böylece kendi endüstriyel araçlarına ait protokollerini geliştirmişler ve ortaya koymuşlardır. Üreticinin cihazında bazen birbirinden ayrı protokoller ile çalışan cihazların aynı anda çalıştığı SCADA sistemlerinin oluşturulması ve kullanılması engellenmektedir. Bunun sebebi ise tek bir tipte protokol desteği sunmasıdır. Bundan dolayı SCADA sistemleri üzerinde herhangi bir değiştirme işlemi yapmak oldukça zordur. Buna ek olarak bu sistemlere yeni cihazları eklemekte oldukça zor bir durumdur.

Sahadaki olayların gözlemlenmesi ve denetlenmesi amacıyla gereken bilgisayar yapı ve uygulama alanları en üstte bulunan katmanda yer almaktadır. Buradaki katman içinde bulunan zaman ağı yapısıyla iletişim kuran donanımsal ve sunucu denetleme yapıları yer

almaktadır. İnsan makine arayüzü (Human Machine Interface- HMI), sahada bulunan ekipmanların gözlemlenmesi ve denetlenmesinde kullanılan grafiksel arayüz yapısıdır. Buradaki arayüz bilgisayarlarda faaliyet gösteren donanımsal birim ve bir programa sahip bir metrik olarak ortaya koyulmuştur. Yazılımsal bir çözüm olarak oluşturulan bu arayüz genel amaç taşıyan bir işletim sisteminde çalışan bir programdır. Bundan dolayı işletim sistemi ve bilgisayar ağ yapısı ve güvenlik açıkları içermektedir. Bu arayüz donanımsal bir çözüm olarak kullanıldığında farklı bir cihazlar bütününe gerek duymadan saha cihazları ile uyumlu bir şekilde çalışan protokolle iletişim kuran bir donanım yapısıdır [70].

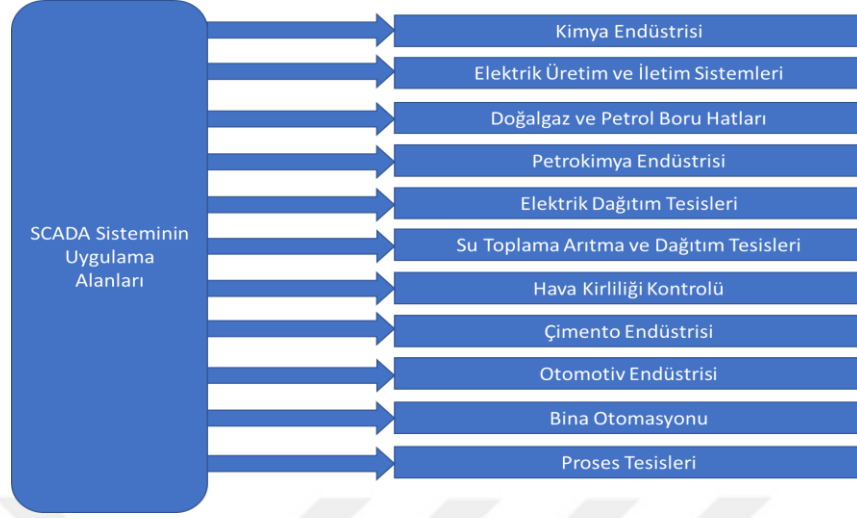
1.1.7.2. Denetim Kontrolü ve Veri Toplama Sisteminin İşlevleri

SCADA birçok işleve sahiptir. Bu işlevler ise aşağıda olduğu gibidir;

- Gözlemleme veya İzleme (Monitoring) İşlev yapıları
- Denetleme İşlev yapıları
- Verileri Bir Araya Getirme İşlev Yapıları
- Verilerin Kaydedilmesi ve Gizlenmesi İşlev Yapıları

1.1.7.3. Denetim Kontrolü ve Veri Toplama Sisteminin Uygulama Alanları

SCADA sisteminin içerisinde bulunan birbirinden farklı birçok kullanım alanı yer almaktadır. Dünyada büyük bir alanda bulunan hem yerel hem de bölgesel birbirinden çeşitli birçok tesiste ortaya çıkmakta ve kullanılmaktadır.



Şekil 1.1.7.3. SCADA sisteminin başlıca uygulama alanları [72]

SCADA sisteminin en ön çıkan kullanım ve uygulama alanları Şekil 1.1.7.3'te verilmiştir. Türkiye'de de birçok SCADA uygulamasına rastlanmaktadır. Buna örnek olarak İstanbul metrolarının içerisinde yer alan yürüyen merdivenler, ışıklandırma sistemleri, havalandırma fanları, yangın koruma ve bildirme sistemleri ve enerji dağıtım sistemleri verilebilir. Bu sistemler tamamıyla bilgisayar ortamlarında izlenmekte ve gerektiğinde ihtiyaç duyulan bütün müdahaleler merkezi kontrol ünitesi adı verilen yapıda uygulanmaktadır.

Yine örnek vermek gerekirse Bolu'da bulunan deprem tehlikesi bulunan konutların elektrik dağıtım yapılarında da SCADA sistemi çok önemli bir yere sahiptir ve çok aktif bir şekilde kullanılmaktadır. Botaş'ın doğal gaz sistemlerinin bütün hatlarında yine SCADA sistemi kullanılmaktadır. Kayseri, Ankara ve İzmir gibi bazı şehirlerde pompa istasyonlarının bulunduğu sistemlerde, ölçüm yapılan bütün noktalarda, Su ve Kanalizasyon İdarelerinin su depolarının kontrolünde SCADA sistemi kullanılmaktadır.

İzmit'te görülmüş 1999 yılı ağustos ayında meydana gelen acı deprem felaketinde SCADA sistemleriyle doğalgaz istasyonunda bir problem ortaya çıkmamıştır. SCADA denetleme odası içinde bulunan şebeke ana çelik vanalar hemen otomatik olarak kapatılmıştır. Bununla birlikte 27 adet bölge içinde bulunan regülatörlerde de eş zamanlı ve koordine bir şekilde durdurulmuştur. Aynı zamanda vana odaları çalışan bütün personeller

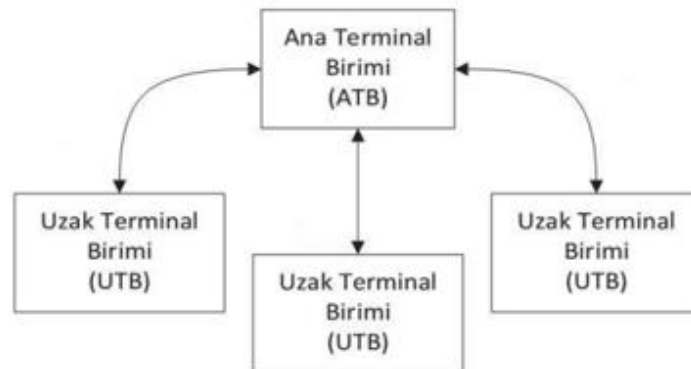
tarafından kapatılmış olmasıyla tüm sistemin gaz akışı kesilmiş büyük bir felaket böyle önlemiştir [71].

1.1.7.4. Denetim Kontrolü ve Veri Toplama Sisteminin Versiyonları

Bilgi teknoloji alanında meydana gelen gelişmelerle beraber birbirinden yeni haberleşme teknolojileri ortaya çıkmıştır. Yeni teknolojik iletişim araçlarının kullanılmasıyla geliştirilmiş olan ürünlerin yetenekleri de artmıştır. SCADA sisteminin büyük bir çevreye yayılmış saha araçları ve merkezi birim ile arasında olması gereken iletişim gelişen teknolojiye paralel bir şekilde ilerleme göstermiştir. Bilgisayar teknolojilerinde çok önemli bir yer tutan haberleşme alt yapı sistemleri, SCADA sistemine paralel bir şekilde uyarlanmıştır. Daha farklı haberleşme alt yapılarını kullanan SCADA sistemi dört farklı şekilde ortaya konulmuştur [69,70].

Seri haberleşme teknolojilerinin kullanıldığı dönemde en iyi haberleşme teknolojileri olarak görülmekteydi. Bu şekilde görülmüş olmalarına rağmen bazı problemleri ortaya çıkmaktadır. Seri haberleşme protokolleri kullanılmıştır. Böylece tek bir noktadan gözlemlene ve denetleme işlerini sağlayan birinci nesil SCADA sistemi ortaya konulmaktadır.

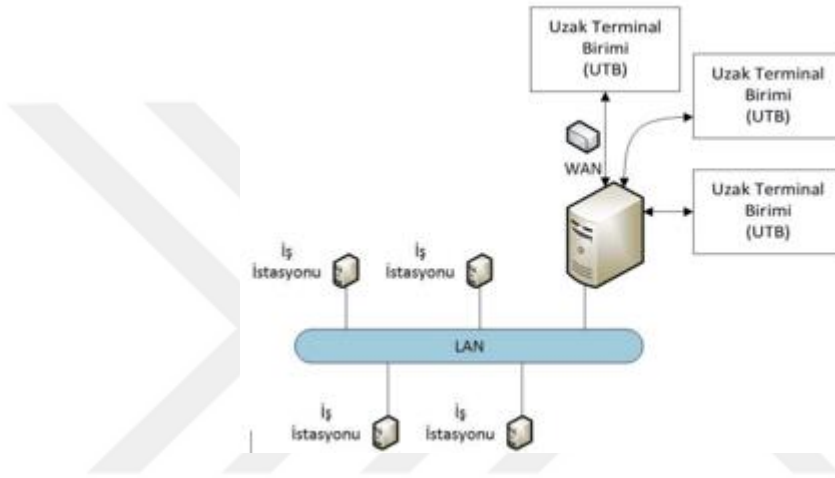
Şekil 1.1.7.4.1’de birinci nesil SCADA sistemi görülmektedir.



Şekil 1.1.7.4.1. SCADA sisteminin birinci nesil versiyonu [70]

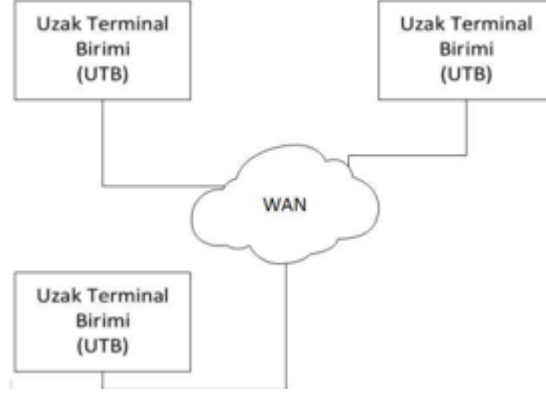
SCADA sisteminin kullanıldığı yerlere göre bazı zamanlarda bir tane izleme ve kontrol merkezi bazen de birden fazla izleme ve kontrol merkezi olması gerekmektedir. Birden çok kontrol ve merkezi izleme merkezinin gerekliliğinden dolayı ikinci nesil SCADA sistemi meydana gelmiştir [70].

Şekil 1.1.7.4.2’de ikinci nesil SCADA sistemi görülmektedir.



Şekil 1.1.7.4.2. SCADA sisteminin ikinci nesil versiyonu [70]

SCADA sisteminin yeni teknolojiler ile kullanılmasıyla daha işlevsel ve kullanışlı bir hale gelmiştir. Bağlantı, kapsama alanı, çevresel elementler gibi olumsuz fiziki koşullar daha kararlı ve sağlam bir şekilde çalışabilecek sistemler tasarlayabilmek adına üçüncü nesil SCADA sistemi geliştirilmiştir [70].

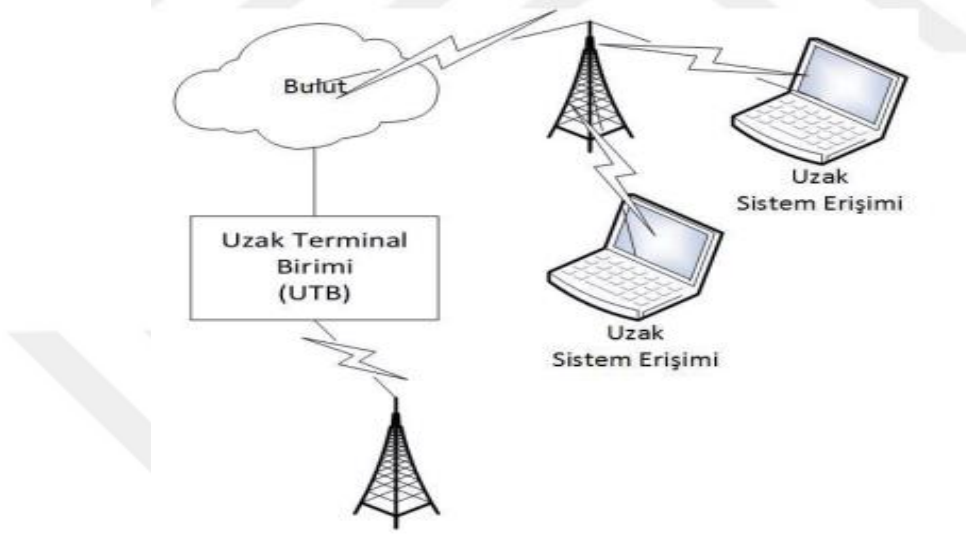


Şekil 1.1.7.4.3. SCADA sisteminin üçüncü nesil versiyonu [70]

Günümüzdeki iletişim altyapısındaki ilerlemeler ve nesnelerin internete bağlanma gereklilikleri nesnelerin interneti (Internet Of Things- IoT) teknolojisini oluşturmaktadır. IoT teknolojisinde iletişim becerisine sahip akıllı nesneler ortamdan elde ettikleri veriyi kontrol ve izleme uygulamalarına aktarmaktadır. Daha sonra ise kontrol yapısından alınan işlemi gerçekleştirmektedir. Ortaya çıkan bu büyük yapının iletişim gerekliliği bulut teknolojisinden elde edilmektedir. Akıllı ev sistem yapıları, akıllı şehir teknolojileri, akıllı şebeke sistemleri, akıllı fabrika yapıları gibi birçok uygulama alanı IoT teknolojisi içinde yer almaktadır [70].

Endüstri 4.0 teknolojisiyle daha büyük kapsama alanı ve daha hızlı iletişim teknolojileri SCADA sistemine entegre edilmiştir. Bunun sonucunda da dördüncü nesil SCADA sistemi ortaya çıkmaktadır.

Şekil 1.1.7.4.4.'de dördüncü nesil SCADA sistemini görmekteyiz.



Şekil 1.1.7.4.4. SCADA sisteminin dördüncü nesil versiyonu [70]

1.1.7.5. Denetim Kontrolü ve Veri Toplama Sistemi Açısından Tehditler

Yerel şirketlerden hükümetlere SCADA sistemini kullanan her kurum ve kuruluş SCADA sistemine özel maalesef tehditlerle karşı karşıya kalmaktadır. Bu tehditlerin sosyal sonuçları olduğu gibi ekonomik sonuçları da oldukça fazladır. SCADA sistemine yönelik bazı tehditler şu şekildedir [73]:

- Hackerler

SCADA ağlarını etkisiz hale getirmek için bireysel ya da ekip halinde çalışırlar. Gün geçtikçe bunların sayısı hızla artmaktadır. SCADA ağını oluşturan bileşenlere sızmaya çalışan hackerler, kurumlara zarar vermek ve savaş başlatmak için uğraşmaktadırlar.

- Zararlı yazılımlar

Virüsler başta olmak üzere fidye yazılımı ve diğer kötü amaçlı yazılımlar SCADA'yı olumsuz yönde etkilemektedir. Bu yazılımlar direkt olarak

SCADA ağını çökertmeye yönelik olmasalar bile SCADA sistemine bağlı altyapılara zarar verebilmektedirler.

- Teröristler

Hackerlardan farklı olarak siber teröristlerin amacı direkt olarak sisteme zarar vermek ve büyük bir kaos çıkartmaktır. Hackerlar genellikle maddi bir beklenti için hareket etmelerine rağmen teröristler direk olarak fikre ve imaja saldırmaktadırlar.

- Çalışanlar

Bazen en büyük zarar, beklenildiği gibi dışarıdan değil içeriden yapılmaktadır. Kötü niyetli olunmasa bile çalışanların yaptığı hatalar SCADA güvenliğini önemli ölçüde etkilemektedir. Ağların büyük olmasına bağlı olarak çalışanların ağ üzerinde çok fazla eylem gerçekleştirmeleri tehlike olasılığını oldukça artırmaktadır.

1.1.7.6. Denetim Kontrolü ve Veri Toplama Sistemi Açısından Saldırılar

İletişim ve bilgi teknolojisinin ilerlemesiyle iletişim, ulaşım yapıları, enerji ve otomasyon teknolojileri gibi önemli sistemler ortaya çıkmaktadır. Buradaki sistemler teknoloji ile her zaman birlikte hareket etmektedir. Bundan dolayı bilgi teknolojilerinde oluşacak olan güvenlik açıkları bilgi teknolojilerinin altyapısını kullanmaktadır. Böylece bu teknolojiler çok önemli altyapı sistemlerini de etkilemektedir. Aynı zamanda bir risk de oluşturmaktadır. Bilgi sistemlerini sarsmak ve ortadan kaldırmak için kullanılan kötü niyetli yazılım uygulamaları önemli alt yapılara da zarar vermektedir.

SCADA sistemi açısından bazı önemli saldırılar vardır. Bu saldırılar [74];

- Sibiry Boru Hattı Patlaması
- The Salt River Proje (SRP) Ele Geçirme Olayı
- Houston Limanı Sistem Arızası
- Slamlere Solucanı
- Kaliforniya Kanal Sisteminin Hecelenmesin
- ABD’de Elektrik Şebekesi Casusluk İhlali

- Nitro Saldırıları
- Tünet Solucanı
- Dugu Truva Atı
- Shamoon Zararlı Yazılımı
- Flame Zararlı Yazılımı
- Doğalgaz Boru Hattı Firmalarına Saldırıları
- Ukrayna Elektrik Kesintisi

SCADA sistemine yönelik saldırılar ile ilgili bir başka tanımda [70,75,76]' da açıklanmıştır. Bu tanıma göre SCADA sisteminde meydana gelen çalışma hataları operatör hatası ve saha cihazı kaynaklarında hatalar olabilmektedir. Ancak bu saldırılar siber saldırı ve kötü amaçlı yazılımlarda olabilmektedir.

1.1.8. Bilgi Teknolojisi Sistemleri ile Denetim Kontrolü ve Veri Toplama Sisteminin Kıyaslanması

Endüstriyel kontrol sistemleri (Industrial Control System- ICS), fiziksel ortamların kontrolünden sorumludur. Bilgi teknoloji (BT) sistemleri ise verilerin toplanması ve yönetilmesinden sorumlu bir yapıdır. ICS yapısının sahip olduğu bazı riskler ve farklılıklar vardır. Bu nedenle geleneksel bilgi teknoloji sistemlerinden farklı karakter özelliğine sahiptir. Buradaki riskler insan yaşamını etkilemektedir. Buna ek olarak bu riskler insan sağlığını ve güvenliğini etkileyen, çevreye ciddi zararlar verilebilen ve üretim kaybına neden olabilen risklerdir. Bu riskler ülkeleri derinden etkileyecek maddi ve yaşamı etkileyen risklerdir. Sistemin yapısında bulunan bu riskler analiz edilmektedir. Bu analiz ile farklı güvenilirlik ve performans gereksinimleri ile karşılaşılmaktadır. Tasarımı yapılan güvenlik tedbirleri sistemin normal akışına zarar vermemektedir. Bununla birlikte siber saldırı anlarında da sistemin bütünlük yapısını koruma altına alacak şekilde uygulanmalıdır [70,77].

ICS ve SCADA sistemi ilk tasarlandıkları zamanlarda, özel bir yazılım ve donanım yapısı kullanılmaktadır. Bu şekilde kendilerine ait protokolleri kolaylıkla çalıştırabilmekteydiler. Bu özelliği ile bilgi teknoloji sistemiyle aralarında çok az bir benzerlik vardı. Hem yaygın bir şekilde kullanılan hem de düşük maddi değerlere sahip

protokollerin ve bilgi teknoloji çözümlerinin ICS'lerde kullanılmaları siber saldırı ve güvenlik açığı riskini oldukça yükseltmektedir. Kurumsal ağ çözümlerine uyumlu olunması ve uzaktan ulaşım yeteneklerinin geliştirilmesi için bilgi teknolojileri çözümleri ICS'lere bütünleştirilmektedir. Bu şekilde dış dünyadan izole bir şekilde tasarlanmış olan ICS'ler keşfedilebilir olmaktadır. Keşfedilebilir bir hale gelen ICS'ler siber saldırılara karşı daha açık bir hale gelmiş olur. Bu nedenle de siber güvenlik çözümlerine ihtiyaç duyulmaktadır. Çevresel faktörlerin sürekli olarak değişkenlik göstermesi ICS uygulamaları için geliştirilmiş olan çözümler BT sistemine karşı geliştirilmiş olan çözümlerden daha farklıdır [70].

BT sistemleri ve ICS'ler arasında gereksinim farkları ortaya çıkmaktadır. Bu farklılıklara Amerikan Birleşik Devletleri Ulusal Standart ve Teknoloji Enstitüsü (National Institute of Standards and Technology) tarafından yayınlanan Endüstriyel kontrol sistemleri rehberliğinde değinilmiştir [78].

1.1.8.1. Performans ve Zamanlama Gereksinimlerine Göre Kıyaslama

Performans ve zamanlama performans ihtiyaçları gözden geçirildiğinde ICS yapısının katı gerçek zamanlı bir şekilde çalıştığı görülmektedir. Çalışma esnasında bazı aksaklıklar ortaya çıkabilir. Bu aksaklıklar sistemin çalışmasını bozabilir. Sistemin çalışması sırasında meydana gelen bu aksamalar katı gerçek zamanlı olarak isimlendirilmektedir. Sistemlerin tasarlanma aşamalarında çalıştıkları hedefe yönelik geç kalma süreleri ortaya çıkmaktadır. Yine bu sistemlerin çalışma çevrelerine göre süreç ayrılıkları görülmektedir. Sahada ölçümü yapılan denetim sinyali ve veri boyutunun ufak olan ICS'lerin büyük ağ yapısı kapasitesi ihtiyacı olduğu ortaya çıkmaktadır. Bilgi teknolojileri sistemlerinin kullanılan uygulamalara göre bazen gerçek zamanlı olma gereksinimi duymaktadır. Bilgi teknolojileri uygulamaları yüksek veri boyutuna ihtiyaç duymaktadır. Bu da yüksek ağ kapasitesi ihtiyacını beraberinde getirmektedir. Gerçek zamanlı işletim sistemleri gerçek zamanlı çalışma ihtiyacına göre çalışmaktadır ve burada ortaya çıkan eksikleri gidermektedir [70].

1.1.8.2. Kullanılabilirlik Gereksinimlerine Göre Kıyaslama

ICS sisteminin saha ortamında yaptığı işler devamlılık özelliğine sahiptir. Akıllı şehirler adı verilen yapılarda şehir alt yapısıyla dağıtım ağına bir enerji girmektedir. Bu enerjinin dağıtım ağı yapısından kullanıcıya gidene kadar kontrol edilmesi ve izlenmesi en iyi devamlılık örneğini oluşturmaktadır. Sahada gerçekleştirilen olayları ve işlemleri denetleyen sistemler asla kopukluğa uğramamaları gerekmektedir. Sistemlerde meydana gelen kopukluklar genellikle günler öncesinden duyurular yapılmaktadır. Bu uyarılar yapılırken programlı ve planlı bir şekilde yapılmalıdır. Bundan dolayı bilgi teknolojileri sistem yapıları (durdurma, yeniden başlatma) erişebilirlik, kesinlik ve bakım gerekliliklerindeki olumlu olmayan etkisinden dolayı kullanılmamaktadır. Bu kesinlik durumu, kararlılık durumu olarak da adlandırılabilir. Kararlılık veya kesinlik durumu sistemin ulaşılabilir olmasına göre belirlenebilmektedir. Sistemin kararlı tutum ortaya koymaması halinde sistem gecikme zamanı farklılığı ortaya çıkmaktadır. Buna bağlı olarak da ulaşılabilirlik gereksiniminde sorunların ortaya çıkması görülecektir [70].

2. YAPILAN ÇALIŞMALAR

2.1. Kullanılan Veri Kümesi

Literatürde yapılan araştırmalar sonucunda diğer çalışmalar ise aşağıda yer alan tabloda olduğu gibidir.

Bu çalışmada ise Siber Fiziksel Sistemlere (Cyber Physical Systems- CPS) yönelik saldırıların kategorize edilmesi amaçlanmaktadır. Bu amaçla, örnek veri seti olarak “A Hardware In The Loop Water Distribution Testbed Dataset For Cyber-Physical Security Testing” çalışmasında sunulan veri seti kullanılmıştır [91].

Burada kullanılan veri seti, üç katmanlı SCADA mimarisinin oluşturduğu ağda toplanmıştır. İletişim protokolleri olarak MODBUS ve TCP/IP protokolleri tercih edilmiştir.

Oluşturulan ağ, fiziksel ve simülasyon olmak üzere iki bölümden oluşmaktadır. Buradaki ilgili ağ üzerinde Ortadaki Adam Saldırısı (Man In The Middle Attack- MITM), Hizmet Reddi Saldırısı (Denial Of Service Attack- DoS) ve tarama saldırısı (Scanning Attack) olmak üzere üç temel sınıfta gerçekleştirilmiş olmakla birlikte gelen ve giden veri örnekleri toplanmıştır.

Bu çalışmadaki sınıflandırma problemi için bir zaman serisi halinde ağ saldırı verisi kullanılmıştır. Bu veri seti tablosu 2.1’ de tanımlanmış olduğu özelliklere sahiptir.

Tablo 2.2. Veri setinin özelliklerinin açıklanması [91]

Sayı	Özellikler	Tanım
1	Src IP Address	Kaynak IP Adresi
2	Dst IP Address	Hedef IP Adresi
3	Src MAC Address	Kaynak MAC Adresi
4	Dst MAC Address	Hedef MAC Adresi
5	Src Port	Kaynak Port
6	Dst Port	Hedef Port
7	TCP Flags	CWR/ECN/URG/ACK/PSH/RST/SYN/FIN Bayraklar
8	Payload Size	Paket yükünün boyutu
9	MODBUS Code	MODBUS fonksiyon kodu
10	MODBUS Value	MODBUS yanıt değeri
11	num_pkts_src	son 2 saniyedeki aynı kaynak adresindeki paket sayısı
12	num_pkts_dst	son 2 saniyedeki aynı hedef adresindeki paket sayısı

Bir saldırı tespit sistemi (Intrusion Detection System- IDS) için ilk aşamada ağ sistemine bir saldırı olup olmadığını belirlemek önemli bir durumdur. Bunu gerçekleştirmek için ikili bir sınıflandırma algoritması kullanılabilir. Ancak saldırı önleme sisteminin (Intrusion Prevention System-IPS) performansını artırmak için yalnızca saldırıyı tespit etmek değil, aynı zamanda saldırı tipini sınıflandırmakta çok önemlidir.

Kullanılan veri seti, saldırı bilgisi (saldırı ve saldırı olmayan) ve alt sınıflarını sağlamaktadır. Bu çalışmada sınıflandırılan saldırılar ise;

- 1- İnternet Kontrol Mesaj Protokolü Saldırısı (Internet Control Message Protocol Attack- ICMP Attack)
- 2- Adres Çözümleme Protokolü Zehirlenmesi (Address Resolution Protocol Spoofing- ARP Spoofing)
- 3- İletim Kontrol Protokolü Seli (Transmission Control Protocol Flood- TCP Flood)
- 4- MODBUS Saldırısı (MODBUS Attack)
- 5- İnternet Protokolü Saldırısı (Internet Protocol Attack)

Burada kullanılan veri setinde hem saldırı hem de saldırı dışı bilgilerden oluşan yaklaşık 16 milyon veri bulunmakta olup, bu çalışmada her bir alt küme arasından 41.403 gözlemden oluşan bir alt küme (yalnızca saldırı durumları arasından) tüm veri kümesindeki yüzdelere göre rastgele seçilmiştir. Rastgele seçimlerin birinci durumunda gözlemlerin %80'i rastgele (her bir alt sınıfın oranı aynı tutularak) eğitim verisi olarak seçilir ve %20'si test verisi olarak kullanılır. İkinci durumda ise gözlemlerin %70'i rastgele (her bir alt sınıfın oranı aynı tutularak) eğitim verisi olarak seçilir ve %30'u test verisi olarak kullanılmaktadır.

Seçilen bu veri setinde yukarıda bahsedildiği gibi 5 farklı saldırı tipi (alt sınıf) bulunmaktadır. Her saldırı türü 1'den 5'e kadar yukarıda olduğu gibi tamsayılar kullanılarak etiketlenmiştir. Daha sonrasında ise saldırı türünü yüksek doğruluk oranı ile tahmin etmek için makine öğrenimi algoritmaları kullanılmıştır. Bu algoritmalar ise;

- Destek Vektör Makinesi (Support Vector Machine- SVM)
- K-En Yakın Komşuluk Algoritması (K-Nearest Neighbors-KNN)
- Karar Ağacı Algoritması (Decision Tree)
- Rastgele Orman Algoritması (Random Forest)
- AdaBoost Algoritması (Adaptive Boosting)

2.2. Çalışmada Kullanılan Yöntemler

2.2.1. Makine Öğrenmesi

Makine öğrenmesi (Machine Learning- ML), genel olarak makinenin zeki insan davranışı ve hareketini taklit etme becerisi şeklinde tanımlanmaktadır. Yapay zekâ sistemleri, karmaşık görevleri, insanların sorunları çözme şeklinde olduğu gibi çözmeye çalışan bir teknolojidir. Bu yönüyle makine öğrenmesi yapay zekanın bir alt alanıdır [92].

Makine öğrenmesi [93]'de ise makinelere minimum insan müdahalesi yaparak kalıpları belirlemek ve tahminler yapmak amacıyla verilerden ve önceki tecrübelerden otomatik bir şekilde öğrenme becerisi sağlayan bir yapay zekâ disiplini olarak tanıtılmıştır. Makine öğrenmesi yöntemleri, bilgisayarların otonom olarak çalışmasını sağlamaktadır. Makine öğrenimi uygulamaları sürekli olarak yeni verilerle beslenmektedir. Bağımsız bir şekilde öğrenebilir, büyüyebilir, geliştirilebilir ve uyarlanabilmektedir. Makine öğrenimi belirli kalıplar elde etmek ve sürekli tekrar eden süreçler için algoritmalarından yararlanarak büyük boyuttaki verilerden anlaşılabilir veriler elde etmektedir. Makine öğrenmesi algoritmaları, bir model olarak hizmet edebilecek önceden belirli olan bir denklemle çalışmak yerine, verilerden doğrudan öğrenmek için hesaplama yöntemlerini kullanmaktadır.

ML algoritmalarının performansı ise “öğrenme” süreçleri sırasında mevcut örneklerin sayısındaki artışla uyumlu olarak çalışmaktadır. Günümüzde büyük veri, IoT ve her alanda kullanılan bilgi işlem teknolojilerinin artması ile makine öğrenimi, çeşitli alanlardaki sorunları çözmek için çok önemli bir yapı haline gelmiştir. ML teknolojisinin kullanıldığı alanlardan birkaç tanesi ise;

- Hesaplamalı Finans (Kredi Puanlama, Algoritmik Ticaret)
- Bilgisayarla Görme (Yüz Tanıma, Hareket İzleme, Nesne Algılama)
- Hesaplamalı Biyoloji (DNA Dizilimi, Beyin Tümörü Tespiti, İlaç Keşfi)
- Otomotiv, Havacılık ve İmalat (Kestirimci Bakım)
- Doğal Dil İşleme (Ses Tanıma)

[94]'de bahsedildiği üzere makine öğrenmesi bir algoritmanın tahminler gerçekleştirirken, bu tahminlerinde daha gerçekçi ve daha doğru olmayı nasıl kavrayıp öğrendiğine göre sınıflandırılmaktadır. Makine öğrenmesi için dört ana yaklaşım vardır. Bu yaklaşımlar ise denetimli öğrenme (supervised learning), denetimsiz öğrenme (unsupervised learning), yarı denetimli öğrenme (semi-supervised learning) ve pekiştirmeli öğrenme (reinforcement learning).

Denetimli öğrenme, etiketli eğitim verileriyle algoritmalar sağlanır. Algoritmanın korelasyonlar için değerlendirilmesi istenen değişkenler tanımlanır. Algoritmanın girdi değerleri belirtildiği gibi çıktı değerleri de belirtilmektedir.

Denetimsiz öğrenme, etiketlenmesi yapılmayan verilerle eğitim verilen algoritma yapılarıdır. Algoritma burada anlamı olan bir bağlantı bulmak için veri kümelerini tarar. Algoritmaların çalıştığı bu veriler, çıktılar, tahminler ve öneriler çok daha öncesinden ortaya koyulmaktadır.

Yarı denetimli öğrenme ise daha önce bahsedilen iki türün bir sentezini içermektedir. Çoğu zaman eğitim verileri bir algoritmayla beslenir. Ancak yarı denetimli öğrenme modelin oluşturduğu bu verileri kendi başına keşfedebilir ve veri kümesine dair kendisine ait bir anlayış geliştirebilir.

Takviyeli öğrenme, bir makineye açık bir şekilde tanımlanmış kuralları olan çok ayaklı bir sürecin tamamlanmasının öğrenilmesi için tipik olarak yinelemeli öğrenmeyi kullanır. Verilen görevlerin tamamlanması için algoritma programlanır ve görevin nasıl tamamlanacağı hakkında olumlu veya olumsuz bilgiler alınır. Algoritma çoğunlukla bu süreçte hangi adımların atılacağına kendi karar vermektedir. Bu makine öğrenme teknikleri bazı görevler için oldukça iyidir.

Denetimli öğrenme (supervised learning):

İkili şekilde sınıflandırma: Verileri ikili şekilde kategoriye ayırma.

Çok sınıflı bir şekilde sınıflandırma: En az ikiden fazla yanıt türü arasından seçimin yapılması.

Regresyon modelleme: Sürekli değerleri tahmin etme.

Birleştirme: Gerçek ve doğru tahmin üretmek amacıyla birden çok makine öğrenmesi modelinin tahminlerini bir araya getirmek.

Denetimsiz öğrenme (unsupervised learning):

Kümeleme: Veri kümesini benzerliğe göre gruplara ayırma.

Anormallik Tespiti: Bir veri setindeki olağandışı veri noktalarının belirlenmesi.

İlişkilendirme madenciliği: Bir veri setinde sıklıkla birlikte meydana gelen öğe setlerinin belirlenmesi.

Boyut azaltma: Bir veri kümesindeki değişkenlerin sayısını azaltma.

Yarı Denetimli Öğrenme (semi-supervised learning):

Makine çevirisi: Tam bir sözcük sözlüğünden daha azına dayalı olarak dili çevirmek için algoritmalar öğretmek.

Dolandırıcılık Tespiti: Yalnızca birkaç olumlu örnek olduğunda dolandırıcılık vakalarını belirleme.

Verileri Etiketleme: Küçük veri kümeleri üzerinde eğitilen algoritmalar, veri etiketlerini daha büyük kümelere otomatik olarak uygulamayı öğrenebilir.

Pekiştirmeli Öğrenme (reinforcement learning):

Robotik: Robotlar, bu tekniği kullanarak fiziksel dünyadaki görevleri yerine getirmeyi öğrenebilir.

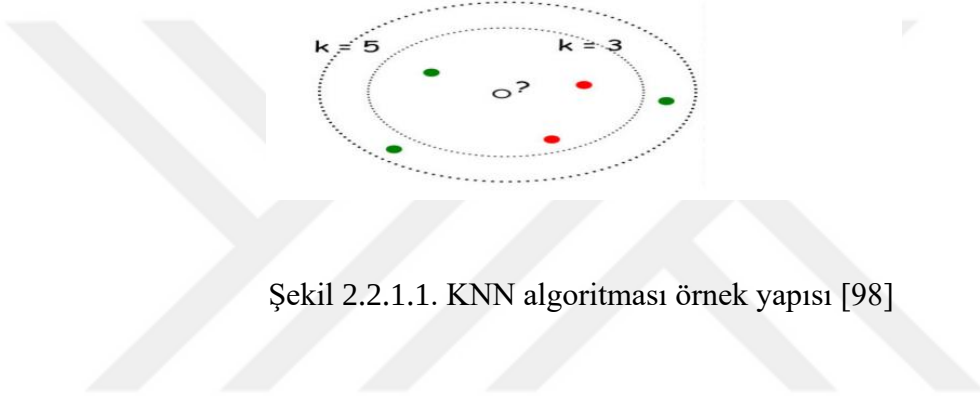
Video Oyunu: Takviye öğrenimi, botlara bir dizi oyunu oynamayı öğretmek için kullanılır.

Kaynak Yönetimi: Sınırlı kaynaklar ve tanımlanmış bir hedef göz önüne alındığında, pekiştirmeli öğrenme, işletmelerin kaynakları nasıl tahsis edeceklerini planlamasına yardımcı olabilir.

2.2.1.1. K-En Yakın Komşu (K-Nearest Neighbors-KNN) ile Sınıflandırma

K-En Yakın Komşuluk Algoritması (K-Nearest Neighbors-KNN), en basit ve en geleneksel parametrik olmayan sınıflandırma algoritmalarından biridir. Girdi vektörlerindeki farklı noktalar arasındaki yaklaşık mesafeleri hesaplar. Daha sonra etiketlenmemiş olan noktayı K en yakın komşu sınıfına atar. KNN sınıflandırıcının üretilmesi sürecinde k önemli bir parametredir ve farklı k değerleri farklı performanslar

sağlamaktadır. k değeri oldukça büyükse, komşular için kullanılan tahmin, büyük bir sınıflandırma süresi yaratacak ve tahminin doğruluğunu etkileyecektir. KNN, örnek tabanlı öğrenme olarak adlandırılmaktadır ve tümevarımsal öğrenme yaklaşımından farklıdır. Bu nedenle, model eğitim aşamasını içermez, sadece girdi ve vektörlerinin örneklerini arar ve yeni örnekleri sınıflandırır. Bu nedenle KNN, “çevrimiçi” örnekleri eğitir ve yeni durumun en yakın komşusunu bulur [95].



Şekil 2.2.1.1. KNN algoritması örnek yapısı [98]

KNN sınıflandırmayı gerçekleştirmek için bir mesafe ölçüm noktasına ihtiyaç duymaktadır. Buradaki probleme özel olarak kullanılabilecek birçok uzaklık ölçüm fonksiyonu bulunmaktadır. Birçok fonksiyona rağmen kullanılabilecek uzaklık ölçüm fonksiyonları ise Öklid, Manhattan ve Minkowski fonksiyonlarıdır.

U ile belirtilen ve mesafeyi göstermek için verilen ilgili fonksiyonlar aşağıda (1), (2) ve (3)’de verilen denklemler ile ifade edilmektedir.

$$U = \sqrt[2]{\sum |x_{training_data} - x_{test_data}|^2} \quad (1)$$

$$U = \sqrt[p]{\sum |x_{training_data} - x_{test_data}|^p} \quad (2)$$

$$U = \sum |x_{training_data} - x_{test_data}| \quad (3)$$

U: Mesafe uzunluğu

$x_{training_data}$: x eğitim verisi

x_{test_data} : x test verisi

p: değişken sayısı

Veri kümesinde de belirtildiği üzere orijinal veri kümesi içinden rastgele seçilen 41.403 gözlem bulunmaktadır. Farklı eğitim veri seti yüzdeleri dikkate alınarak iki farklı analiz yapılmıştır. Birinci durumda gözlemlerin %80'i rastgele (her bir alt sınıfın oranı aynı tutularak) eğitim verisi olarak seçilir ve %20'si test verisi olarak kullanılır. İkinci durumda ise gözlemlerin %70'i rastgele (her bir alt sınıfın oranı aynı tutularak) eğitim verisi olarak seçilir ve %30'u test verisi olarak kullanılır.

Bunların sonucunda KNN algoritması kullanılarak tamsayı değeri verilerek belirtilen saldırılar sınıflandırılmış ve elde edilen doğruluk oranı (Accuracy rates), kesinlik değeri (precision), geri çağırma (recall) ve F1 puan (F1 Score) değerleri aşağıda verilen tablo 2.2.1.1'de gösterilmiştir.

Tablo 2.2.1.1. KNN sınıflandırma sonuçları

	KNN	
70% Eğitim Verisi	Accuracy	61.7181
	Precision	0.8277
	Recall	0.8090
	F1 Score	0.8182
80% Eğitim Verisi	Accuracy	61.9183
	Precision	0.8280
	Recall	0.8106
	F1 Score	0.8192

2.2.1.2. Destek Vektör Makinesi (Support Vector Machine- SVM) ile Sınıflandırma

Destek vektör makinesi (Support Vector Machine- SVM), veri madenciliğinde kullanılan en başarılı algoritmalarından biridir. SVM, hiper düzlemde ikili arama yapmak için yüksek boyutlu alan kullanmaktadır. Karar destek makinesi yaklaşımı, istatistiksel öğrenme teorisine (Statistical Learning Theory- SLT), dayalı bir sınıflandırma tekniğidir. Destek vektör makinelerinin amacı iki sınıf arasındaki ayrım marjını maksimize edecek şekilde doğrusal bir şekilde optimal hiper düzlem bulmaktır. Karar destek makinesi, sistemi eğitmek için bazı verileri kullanmaktadır. Eğitim verilerini temsil eden birkaç destek vektörü bulunmaktadır. Bu destek vektörleri bir SVM modeli oluşturmaktadır. Bu modele göre karar destek makinesi belirli bir bilinmeyen veri setini hedef sınıflara göre sınıflandırmaktadır [96].

Destek vektör makinesi bir veri kümesini kullanarak sınıflandırma, regresyon analizi, örüntü tanıma gibi yöntemleri analiz etmektedir. Giriş ve çıkış olmak üzere iki veri kümesi sınıftan veriler kullanılarak oluşturulmaktadır. SVM’de örnekler noktalarla temsil edilmektedir. Bu örnekler sınıflandırılarak bir model oluşturulmaktadır. Daha fazla kullanılacak numune veri geldikçe kullanılan ortama dahil edilir ve kategorisine göre yerleştirilmektedir [97].

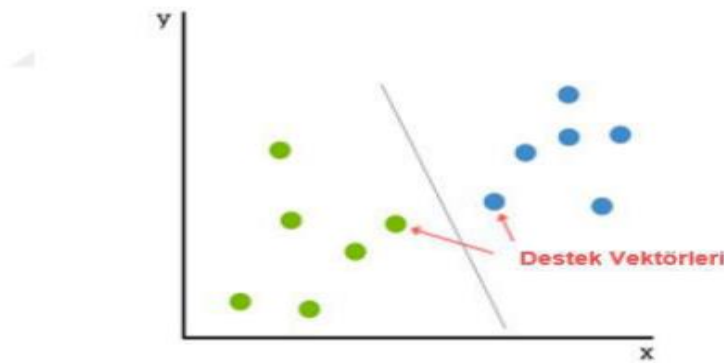
[99]’ da bahsedildiği üzere destek vektör makineleri sınıflandırma problemini çözmek için kullanılan kuvvetli sınıflandırma mekanizmalarıdır. İstatistiksel verilere dayanmaktadır. Destek vektör makineleri herhangi bir öğrenme işleminde, ortaya çıkan olay ve nesnelerin düzenli bir şekilde analiz edilmesi ve tanınmasında regresyon ve sınıflama analizini kullanmaktadır. Aynı zamanda bu denetimli öğrenme modeli olarak da nitelendirilebilir.

Destek vektör makineleri, veri setlerindeki sınıflandırma problemleri çerçevesinde değişkenler arasındaki örüntülerin bilinmediği durumları ele almaktadır. Bundan dolayı da bu tür durumlara karşın ortaya atılmış bir makine öğrenmesi algoritmasıdır. Eğitim verisiyle birlikte öğrenme işlemini gerçekleştirmektedir. Veri setine eklenecek güncel verilerin oluşturduğu kayıtlarla doğru ve gerçekçi tahminler yürütmeye çalışmaktadır. Daha sonra da çıkarım yapmayı amaçlamaktadır. Destek vektör makineleri değişkenlerin miktarı iki boyutlu uzayda lineer doğrusal bir yapıda bulunmaktadır. Üç boyutlu uzay denilen yapıda ise düzlemsel bir yapıdadır. Çok boyutlu uzay yapısında ise hiper-düzlem şeklindedir.

Burada belirtilen birbirinden ayırma yapıları ile veri iki veya daha çok sınıf yapısına ayrılarak sınıflandırma mekanizmasında oldukça kuvvetli olmaktadır [98].

Destek vektör makineleri sınıflandırma işlemi gerçekleştirirken bir düzlem üzerinde belirtilen iki grup arasına bir destek sınırı çizmektedir. Bu şekilde grupları birbirinden ayırmaktadır. Ancak çizilen bu destek sınırının yeri, her iki grupta bulunan üyelere de çok uzak bir yer olarak seçimi yapılmalıdır. Yoksa doğru olmayan bir sınıflandırma olayı gerçekleşmiş olabilmektedir. Bu sınır yapısının çizilmesi aşamasında da destek vektör makineleri tekniği devreye girmektedir. İki sınıf halinde bulunan veri setinde, giriş ve çıkış veri seti olarak iki sınıf oluşturulmaktadır. Destek vektör makineleri, sınıflandırma işlemini yapmak için etiketlenmesi yapılan bir girdi veri seti kullanmaktadır. Eğitim örneklerinin girdileri, doğrusal problem için iki kategoriden bir tanesine eklenmektedir. Çoklu yapıdaki problemlerde olduğu zamanda çoklu kategoriden birine eklenmektedir. Destek vektör makinelerinin oluşturduğu eğitim algoritması, güncel olarak gelen bir örneği kategorize etmek amacıyla bir model oluşturmaktadır. Bu model, uzayda yer alan noktalara benzeyen sınıflandırılmış örnekler halinde çalışmaktadır. Kategorize edilmiş olan bu örnekler, olabildiğince geniş açıda, oldukça açık bir hiper-düzlem ile ayrılmaktadır. Güncel örnekler aynı uzay yapısına eklenerek destek vektör makinesi açısından karar doğrusu çizilerek uzayda yer alan kategorisi tahmin edilmeye çalışılmaktadır.

Bunu aşağıda yer alan şekil 2.2.1.2.'da iki boyutlu destek vektör makinesi örnek uzayı şeklinde görebiliriz.



Şekil 2.2.1.2. İki boyutlu destek vektör makinesi örnek uzayı [98]

Veri kümesinde de belirtildiği üzere orijinal veri kümesi içinden rastgele seçilen 41.403 gözlem bulunmaktadır. Farklı eğitim veri seti yüzdeleri dikkate alınarak iki farklı analiz yapılmıştır. Birinci durumda gözlemlerin %80'i rastgele (her bir alt sınıfın oranı aynı tutularak) eğitim verisi olarak seçilir ve %20'si test verisi olarak kullanılır. İkinci durumda ise gözlemlerin %70'i rastgele (her bir alt sınıfın oranı aynı tutularak) eğitim verisi olarak seçilir ve %30'u test verisi olarak kullanılır.

Bunların sonucunda SVM algoritması kullanılarak tamsayı değeri verilerek belirtilen saldırılar sınıflandırılmış ve elde edilen doğruluk oranı (Accuracy rates), kesinlik değeri (precision), geri çağırma (recall) ve F1 puan (F1 Score) değerleri aşağıda verilen tablo 2.2.1.2.'de gösterilmiştir.

Tablo 2.2.1.2. SVM sınıflandırma sonuçları

	SVM
70% Eğitim Verisi	Accuracy  75.7025
	Precision 0.8026
	Recall 0.8360
	F1 Score 0.8189
80% Eğitim Verisi	Accuracy  79.2158
	Precision 0.8560
	Recall 0.9162
	F1 Score 0.8577

2.2.1.3. Karar Ağacı (Decision Tee) ile Sınıflandırma

Karar ağacı (Decision Tree), ayrık değerli fonksiyonlara yaklaşmak için kullanılmaktadır. Aynı zamanda öğrenilen fonksiyon bir ağaç diyagramı şeklinde ifade edilmektedir. Karar ağaçlarında, girdi için en iyi eşleşmeyi elde etme olasılığı bir ağaç grafiği kullanılarak hesaplanmaktadır. Karar ağaçları, hızlı adaptasyonları, basitlikleri ve yüksek algılama hassasiyetleri sayesinde saldırı tespit sistemlerinde en yaygın kullanılan denetimli öğrenme tekniklerinden biridir. Karar ağaçları, kötüye kullanım tespit sistemlerinde de yaygın olarak kullanılmaktadır. Literatürdeki çalışmalar incelendiğinde

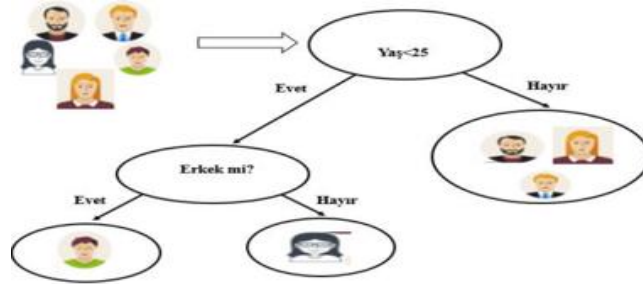
diğer makine öğrenmesi tekniklerine göre yüksek performans sağladığı görülmektedir. Karar ağaçlarındaki düğümler, veri setini herhangi bir özniteliğe göre test etme yeteneğine sahiptir [100].

Düğüm, öznitelik değerlerine göre iki veya daha fazla alt ağaca ayrılmaktadır. Bir m düğüme erişen bir örneğin C_i sınıfında olma olasılığı denklem (3)'de olduğu gibi hesaplanmaktadır.

$$\hat{p} = (C_i \setminus x, m) = p_m^i = \frac{N_m^i}{N_m} \quad (3)$$

Karar ağacı oluşturma ve alt dallara ayırma işlemi safsızlık ölçüsü hesaplanarak yapılmaktadır. Herhangi bir düğüme gelen tüm değerlere aynı içeriğe sahipse, o düğüm saf kabul edilmektedir ve safsızlık değeri olarak 0 alınmaktadır. Safsızlık değerinin 0 olduğu durumlarda, bir düğümü başka alt düğümlere bölmeye gerek yoktur.

[98,101]'de anlatıldığı üzere karar ağaçları, sınıflandırma işlemlerinde oldukça sık kullanılmaktadır. Bu kadar sık kullanılmasının nedeni eğitim ve testin hızlı olmasıdır. Buna ek olarak sonuçlar daha anlaşılırdır, kolaydır ve nettir. Ana fikir, giriş verisinin bir kümeleme algoritmasıyla birlikte tekrarlı yapıda yeni baştan gruplara ayrılmasına ve bölünmesine dayanmaktadır. Gruba ait tüm elemanlar aynı sınıf etiketine sahip olması gerekmektedir. Bu olana kadar kümeleme işlemi devam etmesi gerekmektedir. Bunu şekil 2.2.1.3.'de bir örnek görsel ile görebiliriz.



Şekil 2.2.1.3. İkili karar ağacı yapısı temsili görüntü [98]

Karar ağacı yapısında eşit ağırlığa sahip olasılıklı durumlar yer almaktadır. Bu durumlar büyük belirsizliği ortaya koymaktadır. Bu belirsizliğin en yüksek durumundaki değişkenlik durumu ise maksimum bilgiyi sağlamaktadır. Belirsizliği yok etmek için eğitim ve test verilerinin, durumların doğru ve düzgün bir şekilde tanımlanması gerekmektedir [102].

Karar ağacı ile sınıflandırma işlemleri yapılırken, bu işlemler iki adımda incelenmektedir. Birinci olarak ağaç yapısı meydana getirilmektedir. İkinci olarak ise meydana getirilen bu ağaç yapısından sınıflandırma kuralları oluşturulmaktadır. Karar ağacını temel alan birçok algoritma geliştirilmiştir. Fakat bu algoritmalar düğüm, kök ve dallanma ölçütlerine göre ayrı kategorik sınıflara ayrılmaktadır. Yapılan çalışmalarda çoğu zaman yaygın olarak bilinen ve kullanılan ID3, C4.5 ve C5'tir.

Veri kümesinde de belirtildiği üzere orijinal veri kümesi içinden rastgele seçilen 41.403 gözlem bulunmaktadır. Farklı eğitim veri seti yüzdeleri dikkate alınarak iki farklı analiz yapılmıştır. Birinci durumda gözlemlerin %80'i rastgele (her bir alt sınıfın oranı aynı tutularak) eğitim verisi olarak seçilir ve %20'si test verisi olarak kullanılır. İkinci durumda ise gözlemlerin %70'i rastgele (her bir alt sınıfın oranı aynı tutularak) eğitim verisi olarak seçilir ve %30'u test verisi olarak kullanılır.

Bunların sonucunda karar ağacı algoritması kullanılarak tamsayı değeri verilerek belirtilen saldırılar sınıflandırılmış ve elde edilen doğruluk oranı (Accuracy rates), kesinlik değeri (precision), geri çağırma (recall) ve F1 puan (F1 Score) değerleri aşağıda verilen tablo 2.2.1.3.'te gösterilmiştir.

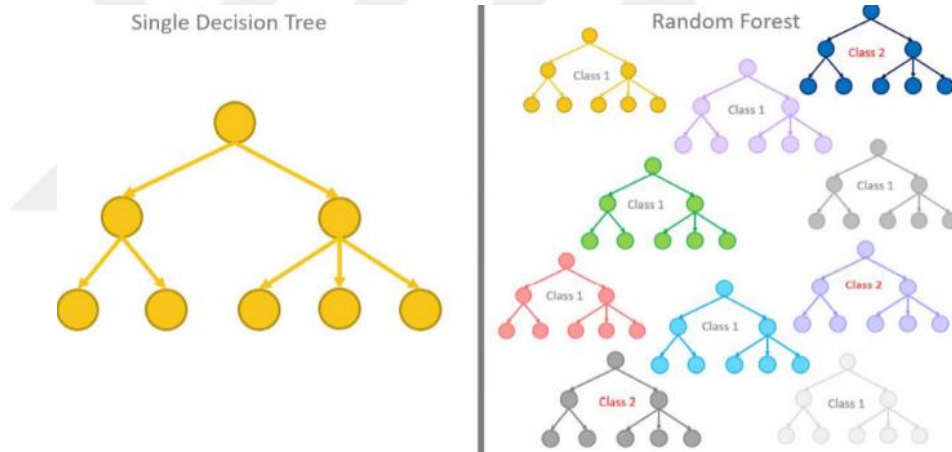
Tablo 2.2.1.3. Decision Tree sınıflandırma sonuçları

	Decision Tree	
70% Eğitim Verisi	Accuracy	98.8380
	Precision	0.9944
	Recall	0.9757
	F1 Score	0.9850
80% Eğitim Verisi	Accuracy	98.8809
	Precision	0.9946
	Recall	0.9766
	F1 Score	0.9855

2.2.1.4. Rastgele Orman (Random Forest) ile Sınıflandırma

Rastgele orman veya rastgele ormanlar (Random Forest) algoritması olarak bilinmektedir. Denetimli sınıflandırma algoritmaları olarak bilinenlerden bir tanesidir. Hem sınıflandırma hem de regresyon sorunlarında kullanılmaktadır. Algoritma birden çok karar ağacı ortaya koyarak sınıflandırma işlemi sırasında sınıflandırma değerini yükseltmeyi amaçlamaktadır. Birbirinden ayrı bir şekilde çalışan birden çok karar ağacının birleşmesiyle aralarında en yüksek skor değeri alanın seçilmesi şeklinde çalışan bir algoritmadır.

Aşağıda yer alan şekil 2.2.1.4.' de bu olay temsil edilmektedir.



Şekil 2.2.1.4. Random forest temsili görüntü [103]

Ağaç sayısı arttıkça net bir sonuç alma oranı yükselmektedir. Karar ağacı algoritması ile arasında fark vardır. Bu fark ise random forest algoritmasının düğümleri bölme işlemini rastgele bir şekilde gerçekleştirme ve kök düğümü bulma şeklinde ortaya koyulmasıdır. Random forest algoritması, elinde yeteri kadar ağaç olması durumunda aşırı öğrenme sorununu azaltmaktadır. Böylece az oranda bir veriye ihtiyaç duymaktadır [103].

[98]'de verilen bilgilere göre random forest algoritması toplu bir şekilde öğrenme metodu olarak açıklanmaktadır. Sınıflandırma seviyesinde birden fazla karar ağacı ortaya

koyarak yüksek sınıflandırma başarısı elde edilmeye çalışılan bir metottur. Rastgele seçilen alt kümelerden tek tek olması koşuluyla oluşturulan karar ağaçları karar ormanı denilen yapıyı meydana getirmektedir. Sonuçları kesin ve hızlı çok fazla sayıda değişkene sahip sorunları kısa zamanda çözüme kavuşturması ve dengesiz veri setlerini kullandığından dolayı birçok alanda başarılı bir algoritma olarak bilinmektedir [104].

Veri kümesinde de belirtildiği üzere orijinal veri kümesi içinden rastgele seçilen 41.403 gözlem bulunmaktadır. Farklı eğitim veri seti yüzdeleri dikkate alınarak iki farklı analiz yapılmıştır. Birinci durumda gözlemlerin %80'i rastgele (her bir alt sınıfın oranı aynı tutularak) eğitim verisi olarak seçilir ve %20'si test verisi olarak kullanılır. İkinci durumda ise gözlemlerin %70'i rastgele (her bir alt sınıfın oranı aynı tutularak) eğitim verisi olarak seçilir ve %30'u test verisi olarak kullanılır.

Bunların sonucunda random forest algoritması kullanılarak tamsayı değeri verilerek belirtilen saldırılar sınıflandırılmış ve elde edilen doğruluk oranı (Accuracy rates), kesinlik değeri (precision), geri çağırma (recall) ve F1 puan (F1 Score) değerleri aşağıda verilen tablo 2.2.1.4.'te gösterilmiştir.

Tablo 2.2.1.4. Random Forest sınıflandırma sonuçları

	Random Forest	
70% Eğitim Verisi	Accuracy	98.7200
	Precision	0.9940
	Recall	0.9740
	F1 Score	0.9820
80% Eğitim Verisi	Accuracy	98,7400
	Precision	0.9940
	Recall	0.9760
	F1 Score	0.9820

2.2.1.5. AdaBoost (Adaptive Boosting) ile Sınıflandırma

AdaBoost, istatistiksel sınıflandırma algoritmalarından biridir. Performansı artırmayı hedeflemektedir. Bunun içinde birden fazla öğrenme algoritmasıyla kullanılmaktadır. Diğer öğrenme algoritmalarının (zayıf öğrenenler) çıktısı veriler, güçlendirilerek oluşturulan sınıflandırıcının en sonuncu çıktısını gösteren ağırlıklı bir toplamda birleştirilerek oluşturulmaktadır. Genellikle, bu algoritma ikili sınıflandırma için kullanılmaktadır. Ancak birçok sınıf ve aralıklarla genişletilmesi mümkündür [105,106].

AdaBoost daha önceki sınıflandırıcılar tarafından yanlış sınıflandırılan örneklerin zayıflıklarını gidermektedir. Bazı problemlerde, diğer öğrenme algoritmalarına göre aşırı uyum sorununa daha az duyarlı olabilmektedir. Bireysel şekilde öğrenenler zayıf olabilirler, ama her bir tanesinin performansı rastgele tahminden biraz daha iyi olduğu sürece, en sonuncu modelin kuvvetli bir öğrenen olduğu sonucu ortaya çıkabilir.

Bütün öğrenme algoritmaları, bazı sorun çeşitlerine göre diğerlerinden daha fazla uyum sağlamaktadırlar. Bir veri setinde en büyük performans ölçütüne ulaşmadan önce ayarlanması gereken çok çeşitli parametrelere ve konfigürasyonlara sahiptirler. AdaBoost genel olarak kullanılmak üzere en hazır şekilde bulunan sınıflandırıcı olmaktadır [107].

AdaBoost, [98,104]'de belirtilen bir diğer tanıma göre de temel sınıflandırıcı yapılarının bir dizi halinde eğitildiği bir yapıdır. Buna ek olarak sıralı bir şekilde sonuçların alınarak tahmin işlemleri için birleştirilmesi olarak da tanımlanmaktadır. Daha sonra da sınıflandırıcının yanlışlarına dikkat ederek bu yanlışların düzeltilmesine ve onarılmasına dikkat kesildiği bir topluluk öğrenmesi metodudur.

AdaBoost algoritmasında ilk olarak birinci ana sınıflandırıcı eğitilmektedir. Daha sonra ise tahminler yapılmaktadır. Bununla birlikte yanlış sınıflandırılması yapılan eğitimlerin ağırlıkları değiştirilmektedir. Daha sonra ise optimize edilmeye çalışılmaktadır. Dizi yapısına ait olan bir çalışma mantığı vardır. Buna göre bir sonra gelen ikinci sınıflandırıcı yapısı ağırlıkları yükselterek kuvvetlendirilmiş eğitim verileri içeri alınmaktadır. Böylelikle işlemler tekrarlı adımlar şeklinde devam etmektedir. Son sınıflandırıcı yapısına kadar bu süreç bu şekilde devam eder. Son olarak elde edilen sonuç başarı oranı ile değerlendirilir.

Veri kümesinde de belirtildiği üzere orijinal veri kümesi içinden rastgele seçilen 41.403 gözlem bulunmaktadır. Farklı eğitim veri seti yüzdeleri dikkate alınarak iki farklı

analiz yapılmıştır. Birinci durumda gözlemlerin %80'i rastgele (her bir alt sınıfın oranı aynı tutularak) eğitim verisi olarak seçilir ve %20'si test verisi olarak kullanılır. İkinci durumda ise gözlemlerin %70'i rastgele (her bir alt sınıfın oranı aynı tutularak) eğitim verisi olarak seçilir ve %30'u test verisi olarak kullanılmaktadır.

Bunların sonucunda AdaBoost algoritması kullanılarak tamsayı değeri verilerek belirtilen saldırılar sınıflandırılmış ve elde edilen doğruluk oranı (Accuracy rates), kesinlik değeri (precision), geri çağırma (recall) ve F1 puan (F1 Score) değerleri aşağıda verilen tablo 2.2.1.5.'te gösterilmiştir.

Tablo 2.2.1.5. AdaBoost sınıflandırma sonuçları

	AdaBoost	
70% Eğitim Verisi	Accuracy	88.3200
	Precision	0.5560
	Recall	0.6000
	F1 Score	0.5740
80% Eğitim Verisi	Accuracy	88.3100
	Precision	0.5560
	Recall	0.6000
	F1 Score	0.5740

3.BULGULAR

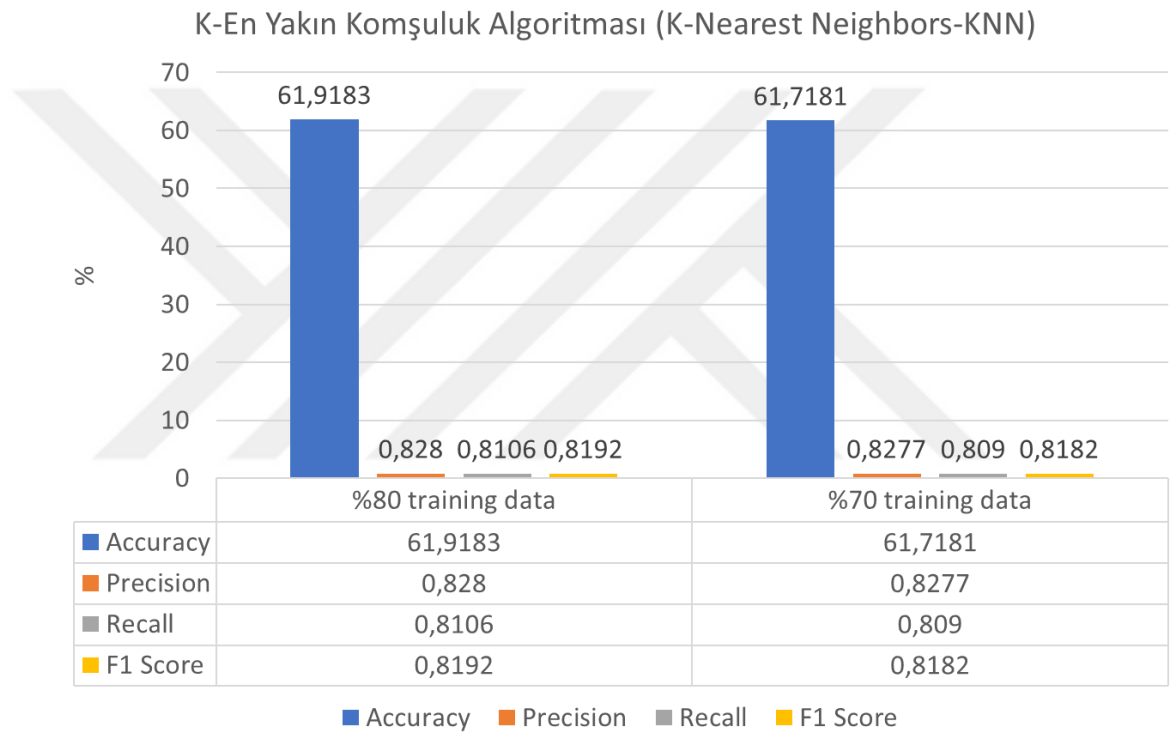
Bu çalışmada sisteme saldırı olup olmadığını belirlemek için kullanılan ikili sınıflandırma yaklaşımı dışında sadece 5 farklı saldırı sınıfı ile bir sınıflandırma problemi ele alınmıştır. 5 farklı makine öğrenmesi yaklaşımı ile veri setinde yer alan saldırılar sınıflandırılmaktadır. Bu makine öğrenmesi yöntemleri en yakın komşu algoritması (K-Nearest Neighbours- KNN), destek vektör makinesi (Support Vector Machine- SVM), karar ağacı (Decision Tree), rastgele orman veya rastgele ormanlar sınıflandırması (Random Forest) ve AdaBoost algoritmasıdır. Sınıflandırma problemi için en iyi performans hem doğruluk oranı hem de izinsiz giriş başına zaman gereksinimi dikkate alınarak karar ağacı (Decision Tree) yaklaşımı ile elde edilmektedir.

Bu çalışmada kullanılan veriler iki farklı durumda gerçekleşmiştir. Birinci durumda gözlemlerin %80'i rastgele (her bir alt sınıfın oranı aynı tutularak) eğitim verisi olarak seçilir ve %20'si test verisi olarak kullanılır. İkinci durumda ise gözlemlerin %70'i rastgele (her bir alt sınıfın oranı aynı tutularak) eğitim verisi olarak seçilir ve %30'u test verisi olarak kullanılmaktadır.

Kullanılan makine öğrenmesi algoritmaları ile sonuçlar grafiksel olarak ifade edilmiştir.

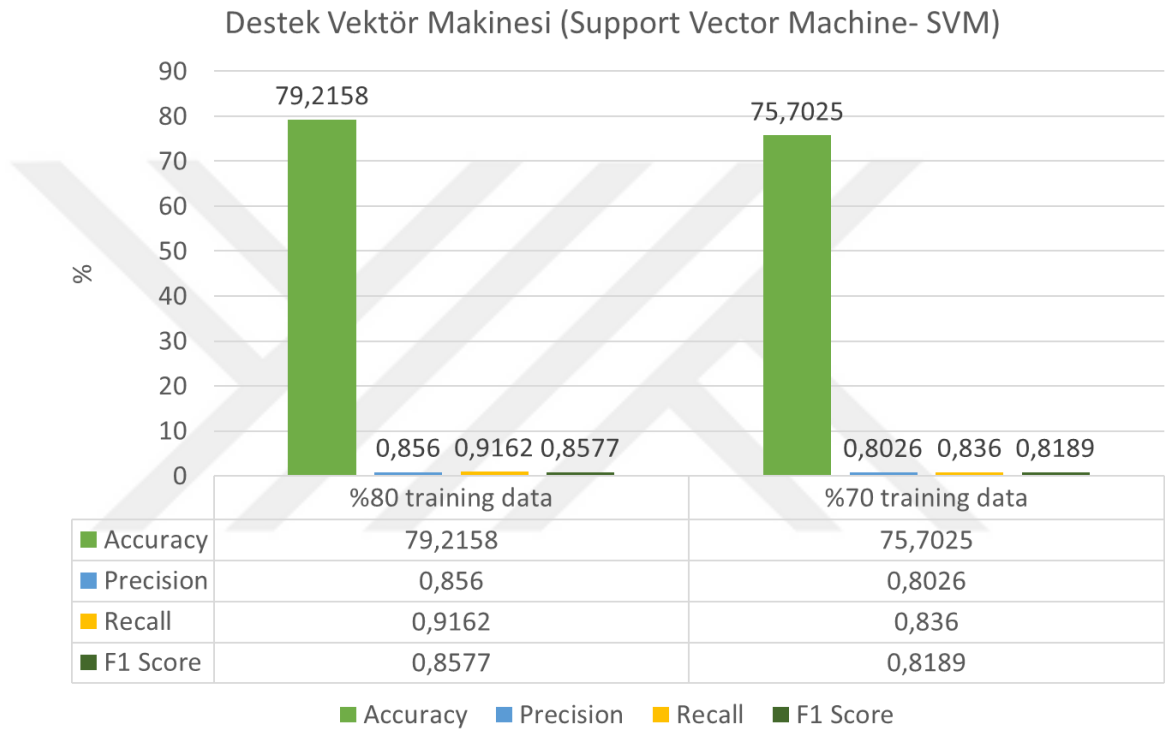
- Destek Vektör Makinesi (Support Vector Machine- SVM)
- K-En Yakın Komşuluk Algoritması (K-Nearest Neighbors-KNN)
- Karar Ağacı Algoritması (Decision Tree)
- Rastgele Orman Algoritması (Random Forest)
- AdaBoost Algoritması (Adaptive Boosting)

1-) K-En Yakın Komşuluk Algoritması (K-Nearest Neighbors-KNN) ile elde edilen doğruluk oranı (Accuracy rates), kesinlik değeri (precision), geri çağırma (recall) ve F1 puan (F1 Score) değerleri aşağıda verilen şekil 3.1’de grafiksel olarak gösterilmiştir.



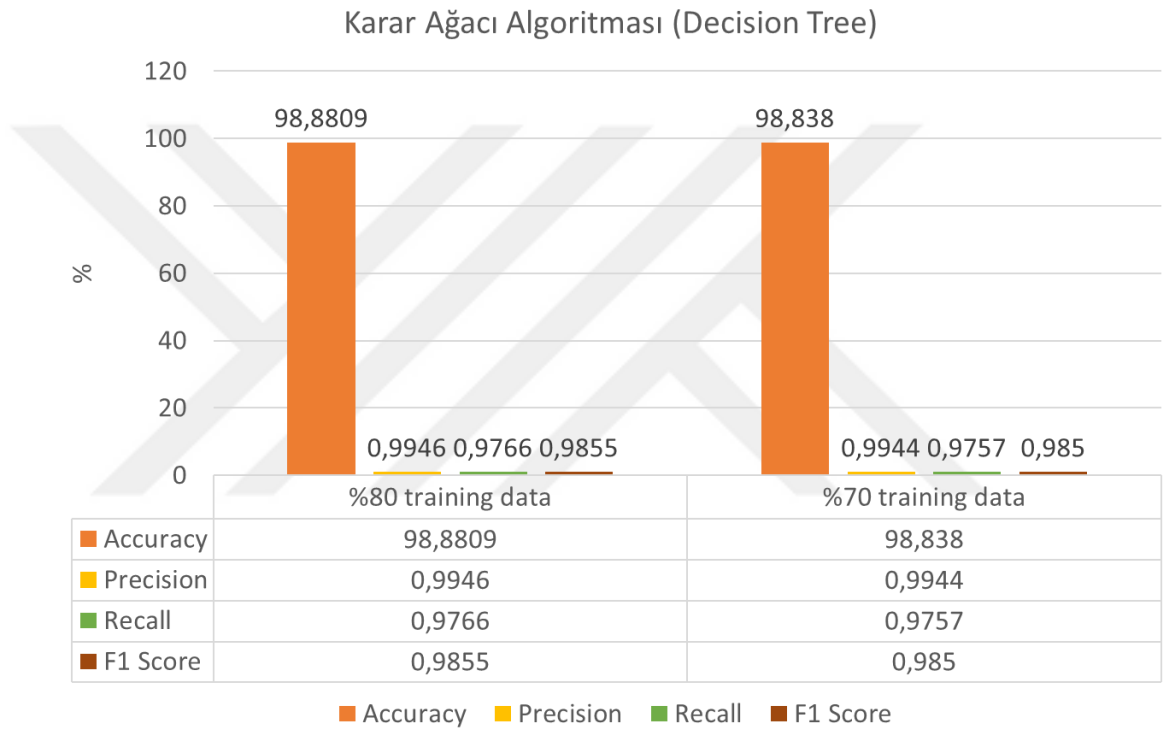
Şekil 3.1. K-En Yakın Komşuluk Algoritması (K-Nearest Neighbors-KNN)

2-) Destek Vektör Makinesi (Support Vector Machine- SVM) ile elde edilen doğruluk oranı (Accuracy rates), kesinlik değeri (precision), geri çağırma (recall) ve F1 puan (F1 Score) değerleri aşağıda verilen şekil 3.2’de grafiksel olarak gösterilmiştir.



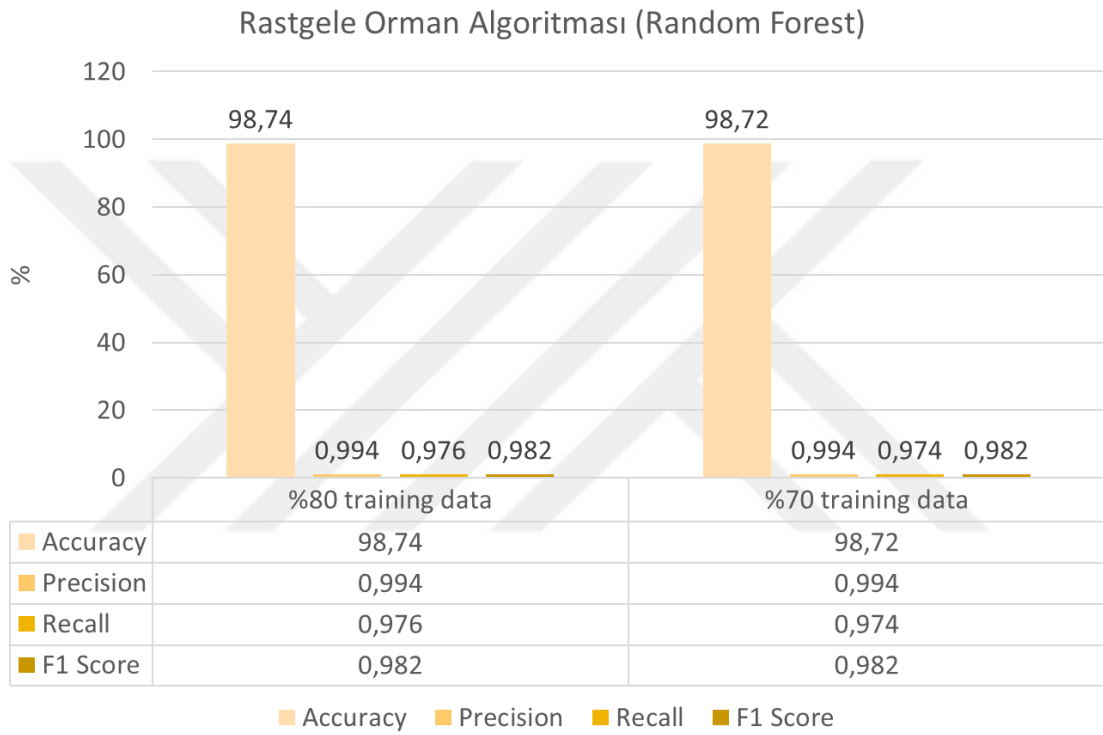
Şekil 3.2. Destek Vektör Makinesi (Support Vector Machine- SVM)

3-) Karar Ağacı Algoritması (Decision Tree) ile elde edilen doğruluk oranı (Accuracy rates), kesinlik değeri (precision), geri çağırma (recall) ve F1 puan (F1 Score) değerleri aşağıda verilen şekil 3.3'te grafiksel olarak gösterilmiştir.



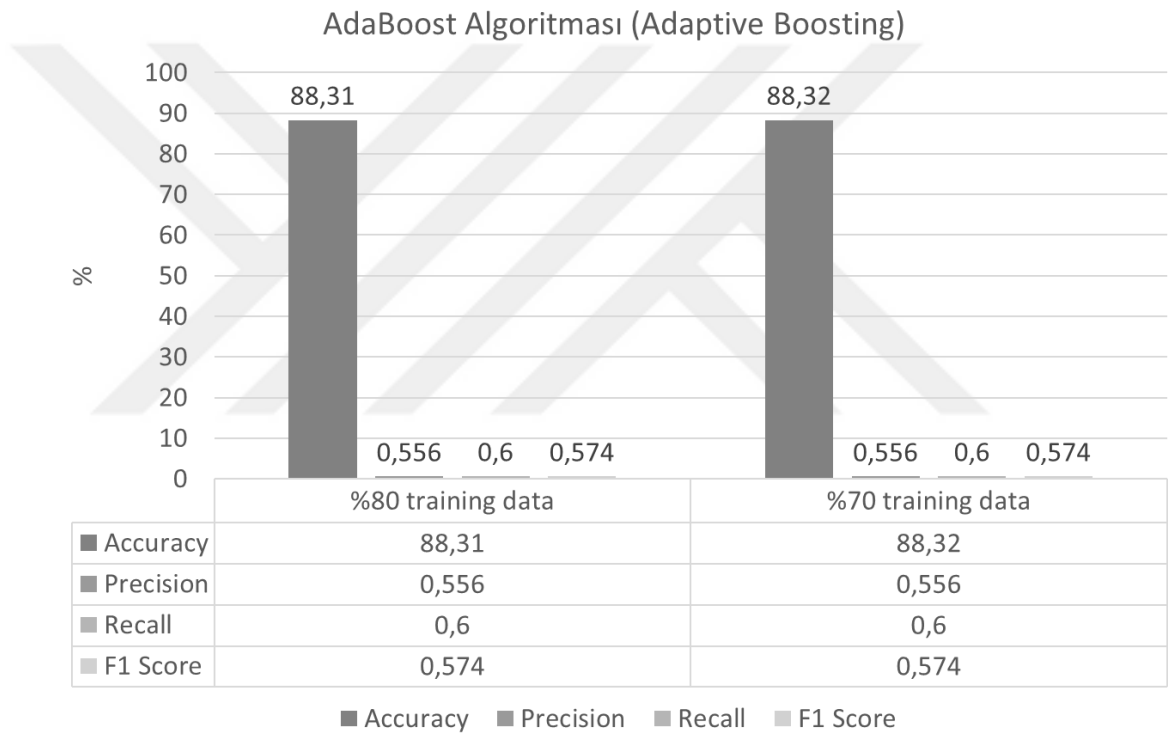
Şekil 3.3. Karar Ağacı Algoritması (Decision Tree)

4-) Rastgele Orman Algoritması (Random Forest) ile elde edilen doğruluk oranı (Accuracy rates), kesinlik değeri (precision), geri çağırma (recall) ve F1 puan (F1 Score) değerleri aşağıda verilen şekil 3.4'te grafiksel olarak gösterilmiştir.



Şekil 3.4. Rastgele Orman Algoritması (Random Forest)

5-) AdaBoost Algoritması (Adaptive Boosting) ile elde edilen doğruluk oranı (Accuracy rates), kesinlik değeri (precision), geri çağırma (recall) ve F1 puan (F1 Score) değerleri aşağıda verilen şekil 3.5'te grafiksel olarak gösterilmiştir.



Şekil 3.5. AdaBoost Algoritması (Adaptive Boosting)

4. SONUÇLAR VE TARTIŞMA

Bilgi teknolojilerinin gelişmesiyle birlikte gündelik hayatımızı birçok kolaylıklar gelmiştir. Günümüzde oldukça yoğun olarak nesnelerin interneti yapısını görmekteyiz. Nesnelerin interneti yapısının gelişmesi kullanılan cihazlarda hem bağlanabilirlik özelliklerinin gelişmesine hem de cihazların akıllı bir yapıya dönüşmesini sağlamaktadır. Nesnelerin interneti teknolojileri sayesinde donanımsal yapıya sahip olan cihazlar çevresel etkenlerin analizini sağlayabilmektedir. Buna bağlı olarak da koşullara göre aksiyon gösterilmekte ve cihazların kontrolünün uzaktan sağlanması gerçekleştirilmektedir.

Geçmişte bu yana bilgisayar ağları oldukça gelişmiştir. Bu gelişme kontrol sistemlerinin bilgisayar ağ tabanlı sistemlere dönüşmesini sağlamıştır. 90'lı yıllardan bu yana kontrol sistemlerinde meydana gelen değişimler sonucunda bazı ürünler ortaya çıkmıştır. Bu ürünlerde denetim kontrolü ve veri toplama sistemi (Supervisory Control and Data Acquisition- SCADA) olarak adlandırılmaktadır. SCADA sistemleri bilindiği üzere endüstri içinde bulunan izleme ve denetleme ihtiyacının çözülmesi amacıyla ortaya çıkan bir yapıdır. SCADA sistemi kullanımı dünya üzerinde giderek artmaktadır. Buna bağlı olarak operasyon maliyetlerinin azalması dünya çapında bu sistemi kullanan şirketlerin mali olarak büyümesine olanak tanımıştır.

SCADA sistemi doğal gaz, elektrik şebekeleri, raylı sistemler ve kimyasal/nükleer tesisler gibi hayati öneme sahip alanlarda sıklıkla kullanılmaktadır. İzleme ve kontrol işlemlerini çok iyi bir şekilde gerçekleştirdiğinden dolayı SCADA sistemi bütün alanlar için çok önemlidir.

SCADA sistemlerine birçok saldırı yapılmaktadır. Bu saldırılara bakıldığında zaman ise bireysel saldırılardan daha çok devletlerin birbirine zarar vermek amacıyla yaptığı saldırılar öne çıkmaktadır. Gürcistan, Ukrayna, Türkiye, Avustralya, İran ve Rusya gibi ülkelerin altyapılarına oldukça büyük saldırılar yapılmaktadır. Bu saldırılar endüstriyel kontrol sistemlerin bir ulusal güvenlik sorunu olduğunu ortaya koymaktadır. Bu saldırılar ise siber saldırılar ismini almaktadır.

SCADA sistemi kapalı devre olarak tasarlanmaktadır. Buna rağmen sahada dağıtık olarak bulunmaları nedeniyle VPN gibi güvenli bağlantılar kullanılarak internet alt yapısı ile haberleşen bir yapıya dönüşmüştür. Bu sistemin internet alt yapısını kullanarak haberleşmeye başlamasından dolayı bu sisteme ve kontrol sistemlerine siber saldırılar

yapılmaktadır. Bilgisayar sistemlerinin ve haberleşme ağlarının zafiyetleri vardır. Bu zafiyetlerde SCADA sistemi zafiyeti olarak adlandırılmaktadır.

IoT ve bulut tabanlı SCADA sistemi erişebilirliği yüksektir. Bundan dolayı da saha kullanımı oldukça geniş bir alana yayılmaktadır. Aynı zamanda bu sistemin işlevselliği de artmaktadır. Yüksek oranda erişebilirlik ve bağlanabilirlik kapasitesi, sistemin dış dünya ile temas yüzeyini artırmaktadır. Temas yüzeyinin artması ve farklı teknolojileri üzerinde barındırmasından dolayı sisteme atak ihtimali de o kadar yüksek olmaktadır. Bu nedenden dolayı IoT bulut tabanlı SCADA sistemi çok daha güvensiz olmaktadır.

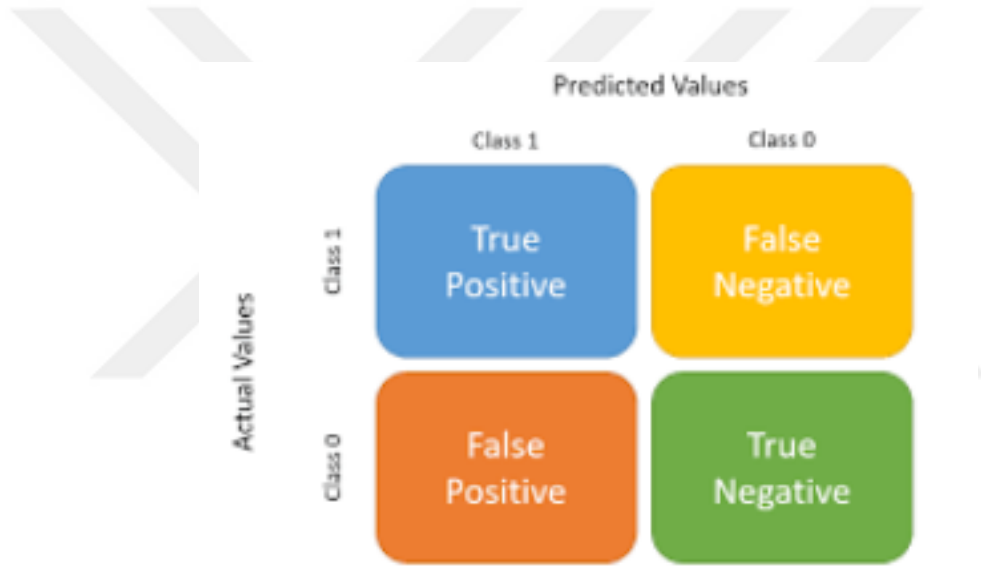
Sonuç olarak bu çalışmada öncelikli olarak siber fiziksel sistemler ile ilgili genel bilgiler verilmiştir. Daha sonra siber saldırı türleri tanımlanmaktadır. Bu tanımlama yapılırken çalışmada adı geçen saldırı türlerinin neler olduğu ve bunların ayrıntılı olarak tanımlarına yer verilmektedir. Daha sonra mevcut çalışmalar ile literatür araştırması gerçekleştirilmiştir.

SCADA sisteminin yapısı, uygulama alanları ve birçok daha özelliği ayrıntılı bir şekilde açıklanmaktadır. SCADA sistemine yönelik saldırıların önemine değinilmiştir.

Bu çalışmada hastaneler ve çeşitli birçok alanda çeşitli açılarda kullanılabilecek bir SCADA sistemi için saldırı tespit algoritması sunulmaktadır. Bu sistem IoT ile bağlantılı ve ortak kullanılabilen bütün endüstriyel alanlarda kullanılabilmektedir. Bu amaçla sistemin eğitimi ve test edilmesi için bir SCADA siber saldırı veri seti kullanılmıştır. Sisteme saldırı olup olmadığını belirlemek için kullanılan ikili sınıflandırma yaklaşımı dışında sadece 5 farklı saldırı sınıfı ile bir sınıflandırma problemi ele alınmıştır. 5 farklı makine öğrenmesi yaklaşımı ile veri setinde yer alan saldırılar sınıflandırılmaktadır. Bu makine öğrenmesi yöntemleri en yakın komşu algoritması (K-Nearest Neighbours- KNN), destek vektör makinesi (Support Vector Machine- SVM), karar ağacı (Decision Tree), rastgele orman veya rastgele ormanlar sınıflandırması (Random Forest) ve AdaBoost algoritmasıdır. Sınıflandırma problemi için en iyi performans hem doğruluk oranı hem de izinsiz giriş başına zaman gereksinimi dikkate alınarak karar ağacı (Decision Tree) yaklaşımı ile elde edilmektedir.

Veri kümesinde de belirtildiği üzere orijinal veri kümesi içinden rastgele seçilen 41.403 gözlem bulunmaktadır. Farklı eğitim veri seti yüzdeleri dikkate alınarak iki farklı analiz yapılmıştır. Birinci durumda gözlemlerin %80'i rastgele (her bir alt sınıfın oranı aynı tutularak) eğitim verisi olarak seçilir ve %20'si test verisi olarak kullanılır. İkinci durumda ise gözlemlerin %70'i rastgele (her bir alt sınıfın oranı aynı tutularak) eğitim verisi olarak seçilir ve %30'u test verisi olarak kullanılmaktadır.

Sonuçları değerlendirmek için performans metrikleri karmaşıklık matrisi (Confusion Matrix) kullanılarak hesaplanmaktadır.



Şekil 4.1. Karmaşıklık Matrisi (Confusion Matrix)

Karmaşıklık matrisi metrikleri ise [108]'de ifade edildiği gibidir.

- Gerçek pozitif (True Positive – TP) – olumlu tahmin ve bu doğru
- Gerçek olumsuz (True Negatif – TN) – Olumsuz tahmin ve bu doğru
- Yanlış pozitif (Yanlış Positive – FP) – olumlu tahmin ve bu yanlış
- Yanlış olumsuz (Yanlış Negatif – FN) – Olumsuz tahmin ve bu yanlış

Karmaşıklık matrisi içerisinde bulunan metriklerin formülleri ise aşağıda (4), (5), (6) ve (7)'de gösterildiği gibidir.

$$\frac{TP+TN}{TP+TN+FP+FN} \quad (4)$$

$$\frac{TP}{TP+FP} \quad (5)$$

$$\frac{TP}{TP+FN} \quad (6)$$

$$\frac{2.(Precision . Recall)}{Precision+Recall} \quad (7)$$

Tamsayı değerleri ile etiketlenen saldırı türleri karmaşıklık matrisi metrikleri ve bu metriklerin ifade edildiği fonksiyonlarla birlikte, destek vektör makinesi (Support Vector Machine- SVM), K-En Yakın Komşuluk Algoritması (K-Nearest Neighbors-KNN), Karar Ağacı Algoritması (Decision Tree), Rastgele Orman Algoritması (Random Forest) ve AdaBoost Algoritması (Adaptive Boosting) yöntemleri ile hesaplanmış ve sonuçları aşağıda verilen şekil 4.2.'de gösterilmiştir.

		KNN	SVM	Decision Tree	Random Forest	AdaBoost
70% Eğitim Verisi	Accuracy	61.7181	75.7025	98.8380	98.7200	88.3200
	Precision	0.8277	0.8026	0.9944	0.9940	0.5560
	Recall	0.8090	0.8360	0.9757	0.9740	0.6000
	F1 Score	0.8182	0.8189	0.9850	0.9820	0.5740
80% Eğitim Verisi	Accuracy	61.9183	79.2158	98.8809	98,7400	88.3100
	Precision	0.8280	0.8560	0.9946	0.9940	0.5560
	Recall	0.8106	0.9162	0.9766	0.9760	0.6000
	F1 Score	0.8192	0.8577	0.9855	0.9820	0.5740

Şekil 4.2. Makine öğrenmesi algoritmalarının genel sonuçları

Şekil 4.2. sonuçlarına göre, öğrenme verisi olarak %80 eğitim verisi kullanıldığında karar ağacı yaklaşımının %98.8809 ile en yüksek doğruluk oranını sağladığı görülmektedir. Eğitim verilerinin farklı yüzdeleri ele alındığında karar ağacı yaklaşımının doğrulukları arasında küçük bir fark görülmektedir. Bu nedenle karar ağacı yaklaşımının eğitim verilerinin %70'i için de uygun olduğu söylenebilir.

Random forest yöntemine göre, öğrenme verisi olarak %80 eğitim verisi kullanıldığında %98.7400 doğruluk değeriyle, karar ağacından daha düşük KNN, SVM ve AdaBoost algoritmalarından ise daha büyüktür. Eğitim verilerinin farklı değerleri ele alındığında random forest yaklaşımının doğrulukları arasında küçük bir fark görülmektedir. Bu nedenle random forest yaklaşımında eğitim verilerinin %70'i kullanıldığında da bu yöntem uygundur ve KNN, SVM ve AdaBoost algoritmalarına göre daha yüksek değer vermektedir.

AdaBoost algoritmasına göre, öğrenme verisi olarak %80 eğitim verisi kullanıldığında %88.3100 doğruluk değeriyle, karar ağacından ve random forest yaklaşımından daha düşük KNN ve SVM algoritmalarından ise daha büyüktür. Eğitim verilerinin farklı değerleri ele alındığında AdaBoost yaklaşımının doğrulukları arasında küçük bir fark görülmektedir. Bu nedenle AdaBoost yaklaşımında eğitim verilerinin %70'i kullanıldığında da bu yöntem uygundur ve KNN ve SVM algoritmalarına göre daha yüksek değer vermektedir.

SVM algoritmasına göre, öğrenme verisi olarak %80 eğitim verisi kullanıldığında %79.2158 doğruluk değeriyle, karar ağacı, random forest ve AdaBoost yaklaşımından daha düşük KNN algoritmasından ise daha büyüktür. Eğitim verilerinin farklı değerleri ele alındığında SVM yaklaşımının doğrulukları arasında küçük bir fark görülmektedir. Bu nedenle SVM yaklaşımında eğitim verilerinin %70'i kullanıldığında da bu yöntem uygundur ve KNN algoritmasına göre daha yüksek değer vermektedir.

KNN algoritmasına göre, öğrenme verisi olarak %80 eğitim verisi kullanıldığında %61.9183 doğruluk değeriyle en düşük değere sahiptir. Eğitim verilerinin farklı değerleri ele alındığında KNN yaklaşımının doğrulukları arasında küçük bir fark görülmektedir. Bu nedenle KNN yaklaşımında eğitim verilerinin %70'i kullanıldığında da bu yöntem uygundur ve yine en düşük doğruluk değerini vermektedir.

Yine bu çalışmada alınan sonuçlara göre, öğrenme verisi olarak %80 eğitim verisi kullanıldığında %0.9855 F1 puan değeri ile en yüksek değere karar ağacı yaklaşımı sahip olmaktadır. Eğitim verilerinin farklı değerleri ele alındığında karar ağacı yaklaşımının F1 puan değerleri arasında küçük bir fark bulunmaktadır. Bu nedenle karar ağacı yaklaşımında eğitim verilerinin %70'i kullanıldığında da yine en yüksek F1 puan değeri görülmektedir.

Öğrenme verisi olarak %80 eğitim verisi kullanıldığında %0.9820 F1 puan değeri ile random forest yaklaşımı karar ağacından daha düşük bir değere sahip olmaktadır. Ancak random forest yaklaşımının F1 puan değeri KNN, SVM ve AdaBoost yaklaşımına göre daha yüksek olduğu görülmektedir. Eğitim verilerinin farklı değerleri ele alındığında random forest yaklaşımının F1 puan değerleri arasında küçük bir fark bulunmaktadır. Bu nedenle random forest yaklaşımında eğitim verilerinin %70'i kullanıldığında da F1 puan değeri karar ağacından daha düşük ama KNN, SVM ve AdaBoost yaklaşımlarından daha yüksek olduğu görülmektedir.

Öğrenme verisi olarak %80 eğitim verisi kullanıldığında %0.8577 F1 puan değeri ile SVM yaklaşımı karar ağacı ve random forest yaklaşımdan daha düşük bir değere sahip olmaktadır. Ancak SVM yaklaşımının F1 puan değeri KNN ve AdaBoost yaklaşımına göre daha yüksek olduğu görülmektedir. Eğitim verilerinin farklı değerleri ele alındığında SVM yaklaşımının F1 puan değerleri arasında küçük bir fark bulunmaktadır. Bu nedenle SVM yaklaşımında eğitim verilerinin %70'i kullanıldığında da F1 puan değeri karar ağacı ve random forest değerinden daha düşük ama KNN ve AdaBoost yaklaşımlarından daha yüksek olduğu görülmektedir.

Öğrenme verisi olarak %80 eğitim verisi kullanıldığında %0.8192 F1 puan değeri ile KNN yaklaşımı SVM, karar ağacı ve random forest yaklaşımdan daha düşük bir değere sahip olmaktadır. Ancak KNN yaklaşımının F1 puan değeri AdaBoost yaklaşımına göre daha yüksek olduğu görülmektedir. Eğitim verilerinin farklı değerleri ele alındığında KNN yaklaşımının F1 puan değerleri arasında küçük bir fark bulunmaktadır. Bu nedenle KNN yaklaşımında eğitim verilerinin %70'i kullanıldığında da F1 puan değeri SVM, karar ağacı ve random forest değerinden daha düşük ama AdaBoost yaklaşımdan daha yüksek olduğu görülmektedir.

Öğrenme verisi olarak %80 eğitim verisi kullanıldığında %0.5740 F1 puan değeri ile AdaBoost yaklaşımı en düşük değere sahip olmaktadır. Eğitim verilerinin farklı değerleri ele alındığında AdaBoost yaklaşımının F1 puan değerleri arasında küçük bir fark bulunmaktadır. Bu nedenle AdaBoost yaklaşımında eğitim verilerinin %70'i kullanıldığında da F1 puan en düşük AdaBoost yaklaşımında görülmektedir.

Buradan alınan sonuçlar ile MITM, DoS ve tarama saldırıları olan sınıf saldırıları dikkate alınarak bu çalışmada aynı veri kümesini (tüm veri kümesini) kullanan yazarlar [91] tarafından sağlanan sonuçlarla karşılaştırılmıştır. Çalışmalarında SVM, KNN ve Random Forest yaklaşımları için saldırı sınıfları sırasıyla %69, %77 ve %75 doğrulukla tahmin edilmiştir. Bu çalışmada ise 41.403 gözlem dikkate alınarak SVM, KNN ve Random Forest yaklaşımları için 5 adet saldırı sınıfları sırasıyla %79.2, %61.9 ve %98.7 doğrulukla tahmin edilmiştir. Aynı zamanda bu çalışmada karar ağacı yaklaşımı ve AdaBoost yaklaşımları da kullanılarak 5 adet saldırı sınıfları sırasıyla %98.8 ve %88.3 doğrulukla tahmin edilmiştir.

Tablo 4.1. Literatür çalışma sonuçları

Yazar / Çalışma	Veri Seti	Yöntem	Doğruluk (Accuracy)	Kesinlik (Precision)	Geri Çağırım (Recall)	F1 Puanı (F1 Score)
Jagtap at al[104]	gas-pipeline	Rastgele Orman	91%	93%	81%	86%
Shitharth at al[105]	ADFA-LD	SVM	74.9%	56.28%	43.53%	49.09%
Jiang at al[106]	Transmission & distribution datasets	SVM	98.47%	99.54%	-	92%
Simon at al[107]	2 Public dataset	SVM	92.53%	-	-	-
		Rastgele Orman	99.84%	-	-	-
Philips at al[108]	Public dataset	SVM	99%	-	-	-
		Karar Ağacı	99%	-	-	-
Rosa at al[109]	gas-pipeline	Karar Ağacı	85%	87%	58%	69%
Muhammed at al[110]	(KDD)-Cap99	KNN	99%	96%	99%	97%
		SVM	98%	100%	97%	98%
Tahir Emre at al[111]	website phishing	AdaBoost	84.45%	82.54%	84.45%	83.01%
		Karar Ağacı	87.46%	87.65%	87.46%	87.45%
		Random Forest	87.93%	87.98%	87.93%	87.87%
		SVM	84.92%	82.61%	84.92%	%82.29
Faramondi at al[112]	WDT dataset	KNN	77%	68%	95%	53%
		SVM	69%	10%	99%	20%
		Rastgele Orman	75%	56%	53%	54%
Tolgahan at al *	WDT dataset *	KNN	61.91%	82.80%	81.06%	81.92%
		SVM	79.21%	85.60%	91.62%	%85.77
		AdaBoost	88.31%	55.60%	60%	57.40%
		Rastgele Orman	98.74%	99.40%	97.60%	98.20%
		Karar Ağacı	98.88%	99.46%	97.66%	98.55%

5. ÖNERİLER

Günümüzde ağ yapıları büyük ve kompleks bir yapıya sahiptir. Bunun yanında çevrede çok fazla çevrimiçi cihaz yer almaktadır. Bu sayede diğer birçok ağa erişim noktasının olmasına bu da siber saldırıların çok yoğun bir şekilde yapılmasına neden olmaktadır. Aynı zamanda siber saldırılar ile saldırı türlerinde de çeşitlilik oluşmaktadır.

Saldırı türlerinin sürekli çeşitlilik kazanması ve ağ yapılarının teknoloji ile birlikte daha fazla sayıya ulaşması da bu yapıların korunmasını bir o kadar zor hale getirmektedir. Saldırının gerçekleşeceği ağları korumak adına alınan anti-virüs koruma yöntemleri ise fayda göstermek konusunda yetersiz kalmaktadır. Bu nedenle saldırı tespit sistemleri yapısını düşünülmesi ve kullanılması kaçınılmaz bir hale gelmiştir.

Saldırı tespit sistemlerinin çalışmasında öncelikle tespit daha sonra da önleme yapılması oldukça önemlidir. Bu nedenle bu sistemlerin çok iyi kurgulanması ve oluşturulması gerekmektedir. Aksi takdirde yapılan saldırıların normal veya normal olmayan saldırı diye tespit edilmesi oldukça zor, hatta imkânsız olacaktır.

Bu çalışmada Siber Fiziksel Sistemlere (Cyber Physical Systems- CPS) yönelik saldırıların kategorize edilmesi amaçlanmaktadır. Bu amaçla, örnek veri seti olarak “A Hardware In The Loop Water Distribution Testbed Dataset For Cyber-Physical Security Testing” çalışmasında sunulan veri seti kullanılmıştır. Bu veri seti bazı saldırı türlerini ve bu saldırı türlerine ait alt saldırı sınıflarını içerisinde bulundurmaktadır.

Bu çalışmada sisteme saldırı olup olmadığını belirlemek için kullanılan yaklaşımda, bir sınıflandırma sorunu sadece 5 farklı saldırı sınıfı ile ele alınmaktadır. Bu saldırıların sayısı alt saldırılarla artırılarak sınıflandırma yapılabilir.

Verilen veri setinde saldırı tipini sınıflandırmak için KNN, SVM, karar ağacı, random forest ve AdaBoost olmak üzere 5 farklı makine öğrenme yaklaşımı uygulanmaktadır. Daha fazla makine öğrenimi algoritması kullanılarak sınıflandırma işlemi yapılabilir. Buna ek olarak derin öğrenme algoritmaları da uygulanarak yine sınıflandırma sonuçlarına bakılabilir.

Yine gelecekteki bir çalışma olarak hem saldırı türlerinin sınıflandırılması hem de normal (saldırı olmayan) veriler makine öğrenmesi yaklaşımları kullanılarak analiz edilebilir.

6. KAYNAKLAR

1. Akben, İ. ve Avşar, İ.İ., Endüstri 4.0 ve Karanlık Üretim: Genel Bir Bakış, Türk Sosyal Bilimler Araştırmaları Dergisi /Journal of Turkish Social Sciences Research, 3,1 (2018) 26-37.
2. Monostori, L., Kádár, B., Bauernhansl, T., Kondoh, S., Kumara, S., Reinhart, G., Sauer, O., Schuh, G., Sihn, V. ve Ueda, K., Cyber-physical Systems In Manufacturing. CIRP Annals, 65,2 (2016) 621-641.
3. Bagheri, B., Yang, S., Kao, H. ve Lee, J., Cyber-physical Systems Architecture for Self -Aware Machines in Industry 4.0 Environment. IFAC-PapersOnLine, 48,3 (2017) 1622-1627.
4. Hellinger, A., ve Seager, H., Cyber-Physical Systems, MacFarlane Business Services and Helen Galloway, National Academy of Science and Engineering, Berlin, 2011.
5. Özahi, E., ÜRGE 506 Endüstri 4.0, Bölüm12 8-16, Gaziantep Üniversitesi Fen Bilimleri Enstitüsü- Ürge ve Tasarım Mühendisliği, Gaziantep, 2019.
6. <http://www.novitek.com.tr/2019/03/25/endustri-tarihine-kisa-bir-yolculuk/>, novitek 27 Ekim 2022.
7. Correia, M. A., Industrie 4.0 Framework, Master's Thesis, The Faculty of Engineering, RheinMain University of Applied Sciences, Rüsselsheim, 2014.
8. Güneş, B., Siber Fiziksel Sistemler Üzerinde Bütünleşik Siber Güvenlik Risk Değerlendirmesi: Bir Konteyner Limanı Uygulaması, Yüksek Lisans Tezi, İ.T.Ü., Fen Bilimleri Enstitüsü, İstanbul, 2019
9. Çeliktaş, B., Siber Güvenlik Kavramının Gelişimi ve Türkiye Özelinde Bir Değerlendirme, Yüksek Lisans Tezi, K.T.Ü., Sosyal Bilimler Enstitüsü, Trabzon, 2016
10. Tungal, T.A., UpGuard, <https://www.upguard.com/blog/cyber-threat> 24 Ekim 2022.
11. <http://www.saglikvebilisim.info/2016/01/25/saglik-sektorunde-siber-guvenlik-tehditler-ve-algilar/> 24 Ekim 2022.
12. Çiftçi, H., Her Yönüyle Siber Savaş (All Aspects of Cyber Warfare), İkinci Baskı, 5-6, TÜBİTAK Popüler Bilim Kitapları, İstanbul, 2017.
13. <https://www.unisys.com/glossary/cyber-attack/>, unisys. 25 Ekim 2022.

14. <https://www.ibm.com/topics/cyber-attack#anchor--84031753>, IBM. 25 Ekim 2022.
15. Hatipoğlu, C. ve Tunacan, T., Türkiye’de Siber Saldırı ve Tespit Yöntemleri: Bir Literatür Taraması, BŞEÜ Fen Bilimleri Dergisi (altı çizili olacak), 8(1), (2021) 430-445.
16. Standler, B. R., Computer crime. <http://www.rbs2.com/ccrime.htm> 25 Ekim 2022.
17. Britz, J., To know or not to know: A moral reflection on information poverty. Journal of Information Science, 30(3), (2004) 193-204.
18. Furnell, S., Cybercrime: Vandalizing the Information Society.
https://link.springer.com/content/pdf/10.1007%2F3-540-45068-8_2.pdf. 25 Ekim 2022.
19. Grabosky, P. ve Smith, R., Crime and the Internet, edited by David S Wall, 29-43, ANU Research Publications, London: Routledge, 2001.
20. Yar, M., The novelty of ‘Cybercrime’ an assessment in light of routine activity theory, European Journal of Criminology, 2(4), (2005) 407-427.
21. Singer, P.W., ve Friedman, A., Siber Güvenlik ve Savaş, 182, Buzdağı Yayınları, Ankara, 2015.
22. <https://blog.turhost.com/siber-guvenlik-nedir/>, turhost. 25 Ekim 2022.
23. https://uludag.edu.tr/dosyalar/bilgiislem/belgeler/siber_guvenlik_nedir.pdf 25 Ekim 2022.
24. Rouse, M., ve Cobb, M., internetofthingsagenda.techtarget:
<https://internetofthingsagenda.techtarget.com/definition/man-in-the-middle-attack-MitM> 26 Ekim 2022
25. Biljana, T., Bogdanoski, M., ve Risteski, A., Handbook of Research on Civil Society and National Security in the Era of Cyber Warfare, 305-351, IGI Global, ABD, 2016.
26. Efe, A., Kalkancı, G., Donk, M., Cihangir, S. ve Uysal, Z., A Hidden Hazard: Man-in-The-Middle Attack in Networks, Anatolian Journal of Computer Science, 4,2 (2019) 98-99.
27. Grimmick, R., Varonis,
<https://www.varonis.com/blog/arppoisoning#:~:text=ARP%20Poisoning%20is%20a%20type,or%20spy%20on%20network%20traffic>. 28 Ekim 2022

28. <https://www.radware.com/security/ddos-knowledge-center/ddospedia/arp-poisoning/>, radware. 28 Ekim 2022.
29. <https://www.wallarm.com/what/arp-spoofing-or-arp-poisoning>, wallarm. 28 Ekim 2022
30. <https://www.geeksforgeeks.org/difference-between-dos-and-ddos-attack/>, geeksforgeeks 28 Ekim 2022
31. <https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/>, cloudflare 28 Ekim 2022
32. <https://www.fortinet.com/resources/cyberglossary/dos-vs-ddos>, Fortinet 28 Ekim 2022
33. <https://berqnet.com/blog/tcp-ip>, Bergnet 29 Ekim 2022
34. <https://www.imperva.com/learn/ddos/syn-flood/>, imperva. 29 Ekim 2022
35. <https://www.privasecurity.com/syn-flood-saldirilari/>, privia. 29 Ekim 2022
36. Errin, Dr. ve Fulp, V., Managing Information Security, Vacca, J.R., Second Edition, 143-175, Syngress, A.B.D., 2014.
37. Bagci, T., G., Sysnettech, <https://www.sysnettechsolutions.com/icmp-nedir/> 29 Ekim 2022
38. <https://www.imperva.com/learn/ddos/ping-icmp-flood/>, imperva. 29 Ekim 2022
39. Koparmal, B., Offensive Cyber Security, <https://bariskoparmal.com/2020/01/13/ddos-saldiri-turleri/> 29 Ekim 2022.
40. <https://en.wikipedia.org/wiki/LAND>, Wikipedia. 30 Ekim 2022.
41. <https://www.imperva.com/learn/ddos/land-attacks/>, imperva. 30 Ekim 2022
42. Silva, A., Reducing Jamming Attack effects, https://www.ktu.edu.tr/dosyalar/36_00_00_0db83.pdf, eprints 30 Ekim 2022
43. <https://www.geeksforgeeks.org/what-are-scanning-attacks/>, geeksforgeeks. 30 Ekim 2022.
44. <https://attack.mitre.org/matrices/enterprise/>, MITRE ATT&CK. 30 Ekim 2022.
45. <https://attack.mitre.org/matrices/enterprise/pre/>, MITRE ATT&CK. 30 Ekim 2022.
46. Susmit, P., Tan, S., J, K.M. and C, M., An experimental evaluation to determine if port scans are precursors to an attack, In 2005 International Conference on Dependable Systems and Networks (DSN'05), June 2005, Yokohama, IEEE, 602-611.

47. Yamashita, T., Miyamoto, D., Sekiya, Y. and Nakamura, H., Slow Scan Attack Detection Based on Communication Behavior, 2020 the 10th International Conference on Communication and Network Security, November 2020, ICCNS 2020, 14-20.
48. <https://www.geeksforgeeks.org/port-scanning-attack/>, geeksforgeeks. 30 Ekim 2022.
49. Lyon, G., Nmap yazılımının Ekran Görüntüsü,
https://tr.wikipedia.org/wiki/Dosya:Nmap_HUN.gif, Wikipedia 30 Ekim 2022
50. <https://tr.wikipedia.org/wiki/Nmap>, vikipedi. 30 Ekim 2022.
51. Bennieston, A.J., NMAP- A Stealth Port Scanner,
<https://nmap.org/bennieston-tutorial/>, nmap.org 30 Ekim 2022
52. <https://www.terabilisim.com/saldiri-tespit-ve-onleme-sistemleri-ips-ids-nedir/>, Tera Bilişim Eğitim ve Danışmanlık. 31 Ekim 2022.
53. Kılıç, H., Katal, N.S. and Selçuk, A.A., Evasion Techniques Efficiency Over The IPS/IDS Technology, 2019 4th International Conference on Computer Science and Engineering (UBMK), November 2019, Samsun, 1.
54. Leng, L. and Wang, L., The fusion method of the IDS and IPS based on IMS, 2012 International Conference on Computer Science and Information Processing (CSIP), September 2012, Xi'an, 1.
55. <https://www.barracuda.com/glossary/intrusion-detection-system>, Barracuda. 31 Ekim 2022.
56. Lutkevich, B., TechTarget - Search Security,
<https://www.techtarget.com/searchsecurity/definition/intrusion-detection-system> 31 Ekim 2022
57. <https://networksimulationtools.com/intrusion-detection-system-projects/>, Network Simulation Tools. 31 Ekim 2022.
58. <https://www.geeksforgeeks.org/intrusion-detection-system-ids/>, geeksforgeeks. 31 Ekim 2022.
59. Liao, H.J., Lin, C.H.R., Lin, Y.C. and Tung, K.Y., Intrusion detection system: A comprehensive review, Journal of Network and Computer Applications, 36,1 (2013) 17-18.
60. <https://www.vmware.com/topics/glossary/content/intrusion-prevention-system.html>, vmware. 1 Kasım 2022.

61. <https://www.forcepoint.com/tr/cyber-edu/intrusion-prevention-system-ips>, forcepoint. 1 Kasım 2022.
62. Georgescu, E., Heimdal Security, <https://heimdalsecurity.com/blog/intrusion-prevention-system-ips/> 1 Kasım 2022
63. <https://www.karel.com.tr/bilgi/saldiri-onleme-sistemi-ips-nedir>, Karel yüz yüze teknoloji. 1 Kasım 2022.
64. Öztürk, T., Saldırı Önleme Sistemi Faydaları, Poweropint 1 Kasım 2022
65. Loshin, P., Techtarget, <https://www.techtarget.com/whatis/definition/SCADA-supervisory-control-and-data-acquisition> 1 Kasım 2022
66. <https://www.samsara.com/guides/scada/>, samsara. 1 Kasım 2022.
67. Gümüş, F., Mühendis Beyinler, <https://www.muhendisbeyinler.net/8-acik-kaynakli-scada-yazilimi/> 1 Kasım 2022
68. Kılıç, M. ve Özdemir, Ş., SCADA Sistemi ile Bir İşletmenin Dış Saha Otomasyonu, AKÜ Fen Bilimleri Dergisi, 10,2 (2010) 60-61.
69. S. Nazir, S. Patel, and D. Patel, “Assessing and augmenting SCADA cyber security: A survey of techniques,” Computers&Security, 70 (2017) 436–454.
70. Yağcı, M.Y., SCADA Sistemler İçin Güvenli Model Oluşturulması, Yüksek Lisans Tezi, İstanbul Üniversitesi-Cerrahpaşa, Lisansüstü Eğitim Enstitüsü, İstanbul, 2020.
71. Akkaya, Ş., Endüstriyel Kontrol Laboratuvarına Ait SCADA Sisteminin Kontrol Programının Gerçekleştirilmesi, Yüksek Lisans Tezi, Marmara Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul, 2010.
72. Öztürk, T., SCADA Sisteminin Başlıca Uygulama Alanları, Poweropint 2 Kasım 2022
73. <https://www.cioupdate.com.tr/connect/nsc/scada-aglarinda-guvenlik-neden-onemli/>, CIO UPDATE. 3 Kasım 2022.
74. Erkek, İ., Modbus Temelli SCADA Sistemlerinin Siber Güvenliği İçin Yeni Bir Yaklaşım, Yüksek Lisans Tezi, Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Ankara, 2018.
75. Akhtar, T., Gupta, B.B. and Yamaguchi, S., Malware propagation effects on SCADA system and smart power grid, 2018 IEEE International Conference on Consumer Electronics (ICCE), January 2018, Las Vegas, 1-6.

76. <https://www.cisa.gov/shields-up>, Cybersecurity&Infrastructure Security Agency. 3 Kasım 2022.
77. Knapp, E. and Langill, J., *Industrial Network Security: Securing critical infrastructure networks for smart grid, scada, and other industrial control systems*. Syngress, 2011.
78. Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M. and Hahn, A., *Guide to Industrial Control Systems (ICS) Security*, 800-82, (Revision 2), 247, Natl. Inst. Stand. Technol. Spec. Publ., ABD, 2015.
79. Sayegh, N., Chehab, A., Elhajj, I.H. and Kayssi, A., "Internal security attacks on SCADA systems", 3rd International Conference on Communications and Information Technology, Communications and Information Technology (ICCIT), June 2013, Lebanon.
80. Hentea, M., *Improving Security for SCADA Control Systems*, InSITE 2008: Informing Science + IT Education Conference, 3, January 2008, ABD.
81. Zhu, B., Joseph, A. ve Sastry, S., *A Taxonomy of Cyber Attacks on SCADA Systems*, "2011 International Conference on Internet of Things", "4th International Conference on Cyber, Physical and Social Computing", iThings/CPSCoM 2011, October 2011, Dalian, 380-388.
82. Davidson, C.C., Yampolskiy, M., Andel, T.R. and McDonald J.T., *On SCADA PLC and fieldbus cyber-security*, 13th International Conference on Cyber Warfare and Security, ICCWS 2018, March 2018, Washington, 140-148.
83. Leverett, E.P., *Quantitatively Assessing and Visualising Industrial System Attack Surfaces*, the degree of MPhil, University of Cambridge, Computer Laboratory Darwin College, Cambridge, 2011.
84. Krotofil, M., Larsel, J. and Gollmann, D., *The process matters: Ensuring data veracity in Cyber-physical systems*, in ASIACCS 2015, Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, April 2015, New York, 133-144.
85. Djouadi, S.M., Melin, M., Ferragut, E.M., Laska, J.A., Dong, J. and Drira, A., *Finite energy and bounded actuator attacks on cyber-physical systems*, 2015 European Control Conference, ECC 2015, July 2015, Linz, 3659-3664.

86. Mitchell, R. and Chen, R., Effect of intrusion detection and response on reliability of cyber physical systems, IEEE Transactions on Reliability, 62,1 (2013) 199-210.
87. Morris, T.H. and Gao, W., Industrial Control System Cyber Attacks, Proceedings of the 1st International Symposium, ICS & SCADA Cyber Security Research, ICS-CSR 2013, September 2013, ABD, 22-29.
88. Bhatia, S., Kush, N., Djamaludin, C., Akande, J. and Foo, E., Practical Modbus Flooding Attack and Detection, Proceedings of the Twelfth Australasian Information Security Conference, January 2014, Auckland, 149, 57-65.
89. Das, A. and Balakrishnan S.G., A Comparative Analysis of Deep Learning Approaches in Intrusion Detection System, 2021 International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT), August 2021, Bangalore, 555-561.
90. Ahn, S., Lee, T. and Kim, K., A Study on Improving Security of ICS through Honeypot and ARP Spoofing, 2019 International Conference on Information and Communication Technology Convergence (ICTC), October 2019, Jeju, 964-967.
91. <https://tools.ietf.org/html/draft-ietf-core-http-mapping-17>. 11.12.2017
92. Clausen, T., Herberg, U., & Philipp, M. (2011). A critical evaluation of the IPv6 routing protocol for low power and lossy networks (RPL). In IEEE 7th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), (pp. 365-372). IEEE.
93. Accettura, N., Grieco, L. A., Boggia, G., & Camarda, P. (2011). Performance analysis of the RPL routing protocol. In 2011 IEEE International Conference on Mechatronics (ICM), (pp. 767-772). IEEE.
94. Burns, A., TechTarget.
<https://www.techtarget.com/searchenterpriseai/definition/machine-learning-ML> 11 Kasım 2022
95. Tasai, C-F., Hsu, Y-F., Lin, C.Y. and Lin, W.Y., Intrusion detection by machine learning, Expert Systems with Applications: An International Journal, 36,10 (2009) 11994-12000.
96. Minnetoğlu, N.A., Makine Öğrenmesi Yöntemleri Kullanılarak Saldırı Tespit Sistemlerinde Performans Analizi, Halic University, 2020.

97. Kaya, Ç., Yıldız, O. and Ay, S., Saldırı tespitinde makine öğrenimi tekniklerinin performans analizi, 24. Sinyal İşleme ve İletişim Uygulama Konferansı (SIU), Mayıs 2016, Zonguldak.
98. Gürmen, C., Saldırı Tespit Sistemleri İçin Makine Öğrenme Yöntemlerinin Performans Karşılaştırılması, Yüksek Lisans Tezi, Harran Üniversitesi, Fen Bilimleri Enstitüsü, Şanlıurfa, 2022.
99. Vapnik, V., Statistical Learning Theory, John Wiley & Sons. Inc., IEEE Transactions On Neural Networks, 10,5, (1998) 988-999.
100. Yayan, U. and Keser, A case study of optimal decision tree construction for RFKON database, 2016 International Symposium on INnovations in Intelligent SysTems and Applications (INISTA), August 2016, Sinaia, IEEE, 1-6.
101. Witten, I.H., Frank, E. and Hall, M.A., DATA MINING: Practical Machine Learning Tools And Techniques, Morgan Kaufmann, 31,1, 192-193, ELSEVIER, Burlington, 2016.
102. Scarfone, K. and Mell, P., Guide to Intrusion Detection and Prevention Systems (IDPS), William Jeffrey, SP 800-94, Revision 1, National Institute of Standards and Technology, Gaithersburg, 2012.
103. Akdağlı, E., Medium.
<https://ece-akdagli.medium.com/makine-%C3%B6%C4%9Frenmesinde-random-forest-algoritmas%C4%B1-a79b044bbb31> 12 Kasım 2022
104. Jagtap, S. S., Sriram, S. and Subramaniaswamy, V., A hypergraph based Kohonen map for detecting intrusions over cyber-physical systems traffic, Future Generation Computer Systems, 119, (2021) 84-109.
105. Shitharth, S. and Prince, W.D., An enhanced optimization based algorithm for intrusion detection in SCADA network, Computers & Security, 70, (2017) 16-26.
106. Jiang, J., Zhao, X., Wallace, S., Sanchez, E.C. and Bass, R., Mining PMU Data Streams to Improve Electric Power System Resilience, BDCAT '17: Proceedings of the Fourth IEEE/ACM International Conference on Big Data Computing, Applications and Technologies, (2017) 95-102.

107. Anton, S.D., Sinha, S. and Schotten, H., Anomaly-based Intrusion Detection in Industrial Data with SVM and Random Forests, 2019 International Conference on Software, Telecommunications and Computer Networks (SoftCOM), (2019).
108. Philips, Brandon., Gamess, E. and Khrisnaprasad, S., An Evaluation of Machine Learning-based Anomaly Detection in a SCADA System Using the Modbus Protocol, ACM SE '20: Proceedings of the 2020 ACM Southeast Conference, (2020) 188-196.
109. Rosa, L., Cruz, T., F, M.B., Quiterio, P., Henriques, J., Caldeira, F., Monteiro, E. and Simoes, P., Intrusion and anomaly detection for the next-generation of industrial automation and control systems, Future Generation Computer Systems, 119, (2021) 50-67.
110. Safari, M., Parvinnia, E. and Haddad, A.K., Industrial intrusion detection based on the behavior of rotating machine, International Journal of Critical Infrastructure Protection, 34, (2021) 100-424.
111. Kalaycı, T.E., Kimlik hırsız web sitelerinin sınıflandırılması için makine öğrenmesi yöntemlerinin karşılaştırılması, Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi, 24,5 (2018) 870-878.
112. Faramondi, L., Flammını, F., Guarino, S. and Setola, R., A Hardware-in-the-Loop Water Distribution Testbed Dataset for Cyber-Physical Security Testing, IEEE, 9, (2021).

ÖZGEÇMİŞ

İlköğrenimini Mehmet Akif Ersoy İlkokulu'nda, orta öğrenimini de yine Mehmet Akif Ersoy İlköğretim Okulu'nda ve lise öğrenimini Vakıfkebir Anadolu Lisesi'nde tamamladı. 2015 yılında Karadeniz Teknik Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü'nde lisans programına başladı ve 2019 yılında bu bölümden mezun oldu. Eylül 2020'de Karadeniz Teknik Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı'nda lisansüstü öğrenimine başladı. Ağustos 2020 tarihinde özel sektör alanında bir firmada Bilgi İşlem Destek Elemanı olarak çalışmaya başladı. Temmuz 2021 tarihinde Haliç Üniversitesi'nde araştırma görevlisi olarak çalışmaya başladı ve Ağustos 2022 tarihinden itibaren İstanbul Üniversitesi-Cerrahpaşa Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü Yazılım Mühendisliği Anabilim Dalı'nda araştırma görevlisi olarak çalışmaya devam etmekte. Evli olan Öztürk yabancı dil olarak iyi seviyede İngilizce bilmektedir.