Afyon Kocatepe Üniversitesi Fen ve Mühendislik Bilimleri Dergisi

Afyon Kocatepe University Journal of Science and Engineering

AKÜ FEMÜBİD **22** (2022) 055102 (1016-1027) AKU J. Sci. Eng. **22** (2022) 055102 (1016-1027)

DOI: 10.35414/akufemubid.1114906

Araştırma Makalesi / Research Article

Bilgisayar Ağlarında Anomali Tespiti Yaklaşımı ile Saldırı Tespiti

Burak EKİCİ[1*], Hidayet TAKCI[2]

[1] *Sivas Bilim ve Teknoloji Üniversitesi, Lisansüstü Eğitim Enstitüsü, Savunma Teknolojileri ABD, Sivas*

[2] *Sivas Cumhuriyet Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği, Sivas*

**Sorumlu Yazar: bekici391@gmail.com* *ORCID ID: https://orcid.org/ 0000-0002-2455-2454*

htakci@cumhuriyet.edu.tr *ORCID ID: https://orcid.org/0000-0002-4448-4284*

Geliş Tarihi: 12.05.2022 Kabul Tarihi: 05.10.2022

Anahtar kelimeler
Saldırı Tespiti; Anomali; Makine Öğrenmesi; Bilgi Güvenliği

Öz

Bilgisayar ağlarına yapılan saldırılar günden güne artarken ve saldırıların nitelikleri de sürekli olarak değişmektedir. Ağ saldırıları, bilgisayar ağlarına zarar vererek bilgi güvenliğini ortadan kaldırmaktadır. Bu durum kişiler, şirketler, kurumlar ve hatta devletler için büyük bir risk oluşturmaktadır. Ağ trafiğinin analizi ve böylece saldırıların ortaya çıkarılabilmesi için Saldırı Tespit Sistemlerinden yararlanılmaktadır. Saldırı türlerini tanıyacak şekilde oluşturulan bu sistemlerin gelişimleri de artan saldırı tiplerine göre sürekli devam etmektedir. Bu çalışmada makine öğrenmesi teknikleri yardımıyla anormallik tabanlı bir saldırı tespit sistemi oluşturulması amaçlanmıştır. Çalışma sürecinde; Yinelemeli Özellik Elemesi, İleri Yönelimli Seçim, Rastgele Orman, Karar Ağaçları, Naive Bayes, Lojistik Regresyon ve Ekstrem Gradyan Artırma gibi algoritmalardan yararlanılmış ve Doğruluk, Kesinlik, Duyarlılık ve F1 gibi metrikler ile değerlendirmeler yapılmıştır. Ayrıca model değerlendirme için ROC eğrilerinden yararlanılmıştır. Bahsi geçen bu algoritmalardan elde edilen sonuçlar karşılaştırılarak en etkili modelin bulunması için CICIDS 2017 veri seti kullanılmıştır. Çalışma kapsamında Yinelemeli Özellik Elemesi ve İleri Yönelimli Seçim teknikleriyle özellik seçimi yapılmış ve en iyi sınıflandırma sonuçları Rasgele Orman ve Ekstrem Gradyan Artırma algoritmalarından elde edilmiştir.

Intrusion Detection on Computer Networks Using Anomaly Detection Approach

Keywords
Intrusion Detection; Anomaly; Machine Learning; Information Security

Abstract

Attacks on computer networks are increasing day by day and characteristics of them are changing continuously. Network attacks destroy information security by damaging computer network systems. This situation poses a great risk for individuals, companies, institutions and even governments. To prevent or minimize the damages of network attacks, Intrusion Detection Systems are used. The development of these systems, which are created according to attack characteristics, continues parallelly to increasing attack types. In this study, it is aimed to create an intrusion detection system based on machine learning principles with anomaly detection. Recursive Feature Elimination, Forward Feature Selection, Random Forest, Decision Tree, Naive Bayes, Logistic Regression and Extreme Gradient Boosting algorithms are used during the study and evaluations are made by Accuracy, Precision, Recall and F1 Score metrics. Also, Cross Validation and ROC Curve methods are used for the evaluation. CICIDS2017 data set is used to find the most effective model by comparing the results obtained from the mentioned algorithms. As the result of this study, it is determined that the Intrusion Detection System models, which are created by classifying the features obtained the methods of Forward Feature Selection and Recursive Feature Elimination with Random Forest and Extreme Gradient Boosting algorithms, are successful.

1. Giriş

Günden güne gelişen teknoloji, her geçen gün daha yoğun bir şekilde hayatın merkezindeki yerini almaktadır. İnsanların konforunun artırılması amacıyla gündelik hayatta ihtiyaç duyulan birçok hizmet internet üzerinden sağlanmaya başlamış ve hatta kullanılan araç-gereçler de internet üzerinden kontrol edilmeye başlanmıştır. İnternet üzerinden alışveriş yapmak, sosyal medya araçları ile birçok kişiyle bağlantı kurmak, internet üzerinden gerçek zamanlı görüntülü görüşmeler ve toplantılar yapmak, yemek sipariş etmek ya da yemek yaparken eksik bir ürünü internet üzerinden sipariş vererek kısa süre içerisinde kapıda teslim almak artık çok kolay hale gelmiştir. Gündelik hayatı kolaylaştıran bu imkânlar, doğal olarak internetin daha fazla kullanıcı tarafından daha yoğun şekilde kullanılması durumunu da ortaya çıkarmıştır. İnternetin yaygınlaşmaya başladığı yıllarda her evde yalnızca bir veya iki internet kullanıcısı varken şu anda bireylerin neredeyse tamamı, üstelik yalnızca bilgisayarlarından değil, cep telefonlarından, tabletlerinden, akıllı saatlerinden vb. cihazlardan ayrı ayrı birer internet kullanıcısı olarak bu büyük trafiğe katılmıştır. Bununla birlikte evlerde bulunan akıllı süpürgeler, buzdolapları, kombiler, kameralar vb. cihazlar da otonom olarak bu internet trafiğinin bir parçasını oluşturmaktadırlar. Oluşan bu devasa boyutlardaki internet trafiği aynı ölçekte veriyi ve verilerin oluşturduğu bilgiyi de bünyesinde barındırmaktadır. Örneğin; internet üzerinden alışveriş yapan bir kişi bu işlem sırasında kullandığı kredi kartı bilgisi gibi hassas verileri internet trafiğine sunmaktadır. Bu örnekteki gibi sadece internet üzerinden alışveriş yapan kişi ile ticaret yapan firma ya da banka arasında gizli kalması gereken verilerin, küresel internet trafiği üzerinde korunması önem arz etmektedir. Sadece bireysel olarak değil daha büyük ölçekte şirketlerin, kurumların ve hatta devletlerin de hassas verilerinin yetkisiz kişilerin eline geçmesi ya da bozulmadan muhafaza edilmesi son derece hayati bir konudur. İnternet trafiği üzerinde bulunan hassas veriler, kötü niyetli insanların iştahlarını kabartmakta ve hassas verilerin yetkisiz insanların eline geçmesi riskini artırmaktadır. İşte bu noktada “Bilgi Güvenliği” kavramı öne çıkmaktadır.

Bilgi Güvenliğinin sağlanmasında çeşitli araçlar, yöntemler ve sistemler kullanılmaktadır. Farklı koşullara ve ihtiyaçlara göre seçilen bu sistemler günden güne gelişmektedir. Saldırı Tespit Sistemleri (STS) de Bilgi Güvenliğinin sağlanması amacıyla kullanılan ve günden güne geliştirilmeye de devam edilen önemli araçlardan biridir. STS de temel amaç belirli bir bilgisayar ağına odaklanarak, ağda meydana gelen trafiğin incelenip yorumlanması ve şüpheli hareketlerin tanımlanarak bunun bir ağ saldırısı olup olmadığının tespit edilmesidir. Bilgisayar ağlarındaki bahsedilen bu şüpheli hareketler ve oluşan olağan dışı trafik anomali olarak adlandırılır. Anomali tespit yaklaşımındaki temel amaç da zaten bu olağan dışı trafiğin tanımlanarak saldırının tespit edilmesidir.

Yapılan bu çalışmada ağ saldırılarının tespitinde başarı oranının artırılması ve yeni saldırı tiplerinin tespit edilmesi amacıyla Makine Öğrenmesi temeline dayalı anomali tespiti yaklaşımıyla bir STS oluşturma amaçlanmıştır. Konuyla ilgili olarak hazır bir veri seti üzerinde özellik seçimi ve sınıflandırma deneyleri yapılmış ve sonuçlar raporlanmıştır.

2. Literatür Özeti

STS, bilgisayar ağlarına yapılan saldırı türlerine göre farklı niteliklere sahip olabilmeleri açısından sürekli değişim ve gelişim halindedir. Saldırı türleri değiştikçe, oluşturulacak olan STS de yeni saldırı türlerini tespit edebilmesi açısından farklı niteliklere gereksinim duyar. Bu nedenle geçmişten beri bu alanda yapılan birçok çalışma mevcut olmakla birlikte yeni çalışmalara ve farklı tekniklere duyulan ihtiyacın da devam etmesi kaçınılmazdır. Geçmişte yapılan çalışmalar incelendiğinde;

Jabez ve Muthukumar (2015) saldırı tespiti konusunda yaptıkları çalışmada Aykırılık Tespiti adını verdikleri yeni bir yaklaşım önermektedir. Bu yaklaşıma göre anomali veri seti Komşuluğa Aykırı Faktör (Neighborhood Outlier Factor) ile ölçülmektedir. KDD veri setinin kullanıldığı bu çalışmada önerilen yaklaşımın var olan saldırı tespit sistemlerine göre daha az yürütme zamanında

çalıştığı ve daha çok anomali veriyi tespit edebildiği ortaya konulmuştur.

Aljawarneh vd. (2018)'e göre etkin bir şekilde ağ saldırılarının tespitinin yapılabilmesi için verilerin son derece hassas bir şekilde toplanması gerekmektedir. Yazarlar, bu çalışmada saldırı kapsamının eşik değerini, ağ işlemlerindeki verilerin eğitim için kullanıma sunulan özelliklerinden en uygun olanlarına göre değerlendirmek için yeni bir hibrit model geliştirmişlerdir. Bu hibrit model J48, Rastgele Orman, Naive Bayes, DecisionStump ve AdaBoost sınıflayıcılarını bünyesinde barındırmaktadır. NSL-KDD veri setindeki anlamlı özelliklerin ortaya çıkarılmasında Bilgi Kazanımı ve Oylama şemaları kullanılarak sonuçta ikili sınıflar için %99,81 ve çoklu sınıflar için ise %98,56'lık oranda saldırıları doğru tespit etme başarısı yakalanmıştır.

Yıldırım vd. (2014) ise yaptıkları çalışmada KDD Cup 99 veri seti üzerinde çok katmanlı yapay sinir ağı kullanarak bir STS modeli oluşturmuşlardır. Oluşturulan modelin eğitim setindeki başarısı %99, test setindeki başarısı ise %90,61 olarak ölçülmüştür.

Alamiedy vd. (2019) yaptıkları çalışmada Çok Katmanlı Gri Kurt Optimizasyon Algoritmasını kullanarak NSL-KDD veri setindeki en anlamlı özellikleri seçmiş ve çeşitli sınıflayıcılarla bir STS modeli oluşturmuşlardır. Çalışma sonucunda veri setindeki özellik sayısının azaltılmasının başarı oranını artırdığı gözlenmiştir.

Chen vd. (2017) yeni saldırı tiplerinin tespiti için denetimsiz öğrenme tekniklerine dayalı bir STS yaklaşımını önermişlerdir. Çalışmanın kümeleme aşamasında DBSCAN, One-SVM, Agglomerative Clustering ve Expactation-Maximization modelleri kullanıldıktan sonra oylama modeli ile tutarlı sonuçlar elde edilmiştir. Çalışma sonucunda Hatalı-Pozitif (FP) metriğine göre geleneksel yöntemlere oranla önerilen sistemin daha başarılı olduğu görülmüştür.

Kumar vd. (2020) tarafından CICIDS 2017 veri seti üzerinde yapılan çalışmada Rastgele Orman algoritmasına dayalı olarak özellik seçimi yapılmış ve ardından Karar Ağacı, Çok Katmanlı Yapay Sinir Ağı, Naive Bayes ve Topluluk Öğrenmesi algoritmaları ile sınıflandırmışlardır. Çalışma sonucuna göre en yüksek sınıflandırma doğruluğu Karar Ağacı algoritmasıyla elde edilmiştir.

Ran vd. (2019) Aegean Wi-Fi Intrusion Dataset (AWID) veri seti üzerinde hem denetimli öğrenme hem de denetimsiz öğrenme teknikleri kullanarak iki aşamalı bir saldırı tespit sistemi önermişlerdir. Çalışmanın ilk aşamasında daha önce etiketlenmiş veriler denetimli öğrenme teknikleri ile ikinci aşamasında ise etiketsiz veriler denetimsiz öğrenme teknikleri ile değerlendirilmiştir. Çalışma sonucunda ortaya çıkan %98,54'lük genel başarı oranı bu karma modelin başarısına etki etmiştir.

Satam ve Hariri (2020) yaptıkları çalışmada kablosuz ağlarda saldırı tespiti yaparken anomali davranış analizi yaklaşımıyla yüksek doğruluk oranı elde edebileceklerini göstermişlerdir. İlgili çalışmada Arizona Üniversitesi kablosuz ağlarından alınan yerel veri setleri üzerinde n-gram analizi yöntemi kullanılarak yanlış tespit oranını 0,0174 gibi çok düşük bir orana indirgemişlerdir.

Abdel-Aziz vd. (2013) yaptıkları çalışmada iletişim ağlarındaki anomalilerin tespitinde genetik algoritmaları ve Temel Bileşen Analizi (PCA) kullanılarak veri setlerindeki en anlamlı özelliklerin ortaya çıkarılması gerektiğini savunmuşlardır. Ortaya çıkarılan özelliklere dayalı olarak sınıflandırma yapıldıktan sonra NSL-KDD veri seti üzerinde daha önceden bilinen saldırılarda en etkili sınıflayıcının Naive Bayes, tanımlanmamış saldırıların tespitinde en etkili sınıflayıcının ise J48 olduğunu ortaya koymuşlardır.

Jose vd. (2018) yaptıkları çalışmada saldırı tespit sistemlerinde anomali tespit yaklaşımı ve bu yaklaşımın nasıl uygulanabileceği hususunda çeşitli bilgilere yer vermişlerdir. Mevcut tekniklerin incelendiği çalışmada, saldırı tespit sisteminin kullanım yeri ve sistemden beklentilere göre doğru tekniğin seçilmesinin önemi vurgulanmıştır. Saldırı tespit sistemlerinde anomali tespiti yaklaşımının en

büyük avantajının yeni saldırı tiplerinin sisteme tanımlanmasına gerek olmadığı hususu üzerinde durulmuştur.

Karataş ve Şahingöz (2018) ise yapay sinir ağları tabanlı, çok katmanlı bir saldırı tespit sistemi oluşturarak KDD Cup 99 veri seti üzerinde "trainc, trainlm, trainbfg, trainscg, traincgp, trainoss, trainbr, trainr" eğitim fonksiyonlarının karşılaştırmasını yapmışlardır. Doğru-Pozitif (TP) metriğinin ölçek olarak kabul edildiği çalışmanın sonucuna göre en hızlı uygulama zamanı "trainscg" fonksiyonu ile, en düşük hata oranı ise "trainlm" fonksiyonu ile elde edilmiştir.

Zhou vd. (2020) özellik seçimi ve topluluk öğrenmesine dayalı sınıflayıcıları temel alarak verimli bir saldırı tespit sistemi üzerinde yoğunlaşmışlardır. Çalışmanın özellik seçimi aşamasında Korelasyon Tabanlı Özellik Seçimi (CFS) ve Yarasa Algoritması (BA) beraber kullanılmıştır. CFS, sezgisel değerlendirmelerin sonuçlarına göre özelliklerin seçildiği klasik bir filtre algoritması olup, BA ise küçük yarasaların ekolojik konumlanma davranışlarından esinlenerek oluşturulan bir algoritmadır. Sınıflandırma aşamasında ise C4.5, Rastgele Orman ve Cezalandırılan Özellikler ile Karar Ağacı algoritmaları kullanılmıştır. CICIDS 2017 veri seti üzerinde yapılan çalışmada belirtilen algoritmalar ayrı ayrı ve daha sonrasında ise topluluk halinde kullanılarak sonuçlar değerlendirilmiştir. Sonuçlar değerlendirildiğinde, yapılan bu çalışmanın en iyi sonucunun topluluk öğrenme algoritmalarıyla sağlandığı ortaya konulmuştur.

Shaukat vd. (2020) yaptıkları çalışmada, ağ güvenliği ve saldırı sınıflandırmasında kilit rol oynayan makine öğrenmesi tekniklerinden Naive Bayes ve J48 Karar Ağaçları algoritmalarını karşılaştırmışlardır. CICIDS 2017 veri seti üzerinde gerçekleştirilen çalışmanın ilk aşamasında, veri setindeki tüm özellikler herhangi bir eleme işlemine tabi tutulmadan kullanılmış, ikinci aşamada ise Sarmalayıcı Özellik Seçimi tekniğine göre veri setini 8 özellik seçerek indirgemişlerdir.

Fernandez ve Xu (2019) hem denetimli ağ saldırı tespitinde hem de denetimsiz anomali tespitinde derin öğrenmenin kullanılmasıyla ilgili bir çalışma yapmışlardır. Yazarlar öncelikli olarak ileri beslemeli tam bağlı bir derin sinir ağı oluşturarak (DNN) denetimli öğrenme yolu ile ağ saldırı sistemini eğitmeyi daha sonra ise etiketlenmemiş zararlı ağ trafiği verilerini ise denetimsiz öğrenme yoluyla bir otomatik kodlayıcı ile sınıflandırmayı amaçlamışlardır. CICIDS 2017 veri setinin kullanıldığı çalışmada Derin Sinir Ağının (DNN) saldırı tespitinde diğer makine öğrenmesi tekniklerinden daha iyi bir performans sağladığı ortaya çıkarılmıştır.

3. Materyal ve Metot

Literatürde bahsi geçen çalışmalar, makine öğrenmesi tekniklerinin bilgisayar ağlarına yapılan saldırıların tespit edilmesinde kullanılmasının bu alanda başarıyı artırma hususunda güçlü bir potansiyelinin olduğunu göstermektedir. Saldırı türlerinin günden güne değişmesi ve makine öğrenmesi tekniklerinin de geniş yelpazesi nedeniyle bu alanın sürekli olarak yeniliğe ve gelişime açık olduğu görülmektedir. Etkin ve verimli bir saldırı tespit sistemi oluşturmak için anomali tespiti yaklaşımıyla saldırıların tespitinin sağlanması prensibinin benimsendiği bu çalışma ise içerdiği makine öğrenimi teknikleri ve hibrit öznitelik seçimiyle bu alanda daha sonra yapılacak çalışmalarda araştırmacılara fikir verecektir. Çalışmanın temel aşamaları şu şekilde sıralanabilir:

- Veri setinin ön işlemden geçirilmesi
- Sınıflandırma için en uygun özniteliklerin seçimi
- Verilerin sınıflandırılması
- Sonuçların değerlendirilmesi

Çalışma sürecinde yapılan tüm deneyler "Python" dilinde "Spyder" tümleşik geliştirme ortamında gerçekleştirilmiştir.

3.1 Veri Seti

Çalışmada, Kanada Siber Güvenlik Enstitüsü tarafından oluşturulan ve güncel saldırı senaryolarını bünyesinde barındıran Canadian Institute of Cybersecurity Intrusion Detection System 2017 (CICIDS2017) isimli veri seti kullanılmıştır. CICIDS2017 boyutu ve içeriği ile ağ saldırılarının önlenmesi hususunda oluşturulacak olan yeni modellerin ve algoritmaların analizi açısından yeterli bir veri setidir. Veri seti, toplamda 8 ayrı dosyadan oluşmakta ve Kanada Siber Güvenlik Enstitüsünün 5 günlük normal ve saldırı durumundaki ağ trafiğinin kayıtlarını içermektedir. Çizelge 1'de veri setini oluşturan dosyalar hakkında kısa bilgiler görülmektedir.

Çizelge 1. Veri setinde bulunan dosyalar.

Dosya Adı	Günlük Aktivite	Oluşan Aktivite
Monday-WorkingHours.pcap_ISCX.csv	Pazartesi	Normal ağ trafiği
Tuesday-WorkingHours.pcap_ISCX.csv	Salı	Normal ağ trafiği ve FTP-Patator, SSH-Patator saldırıları
Wednesday-workingHours.pcap_ISCX.csv	Çarşamba	Normal ağ trafiği ve DoS GoldenEye, DoS Hulk, DoS Slowhttptest, DoS slowloris, Heartbleed saldırıları
Thursday-WorkingHours-Morning-WebAttacks.pcap_ISCX.csv	Perşembe	Normal ağ trafiği ve Web Attack – Brute Force, Web Attack – Sql Injection, Web Attack – XSS saldırıları
Thursday-WorkingHours-Afternoon-Infilteration.pcap_ISCX.csv	Perşembe	Normal ağ trafiği ve Infiltration saldırısı
Friday-WorkingHours-Morning.pcap_ISCX.csv	Cuma	Normal ağ trafiği ve Bot saldırısı
Friday-WorkingHours-Afternoon-PortScan.pcap_ISCX.csv	Cuma	Normal ağ trafiği ve PortScan saldırısı
Friday-WorkingHours-Afternoon-DDos.pcap_ISCX.csv	Cuma	Normal ağ trafiği ve DDoS saldırısı

Çizelge 1'de gösterilen bu dosyalar birleştirildiğinde 3119345 örnek, 1'i normal ağ trafiğini gösterir şekilde toplam 15 adet sınıf etiketi ve 83 farklı özniteliği bünyesinde barındıran geniş bir veri seti ortaya çıkmaktadır (Panigrahi ve Borah 2018). Etiketlenmiş 15 adet sınıfa ait veri setinde örneği bulunan kayıtların dağılımı da Çizelge 2'de görülmektedir.

Çizelge 2. Veri setinde örnek dağılımları

Sınıf Etiketi	Örnek Sayısı
BENIGN (Normal)	2359087
DoS Hulk	231072
PortScan	158930
DDoS	41835
DoS GoldenEye	10293
FTP-Patator	7938
SSH-Patator	5897
DoS slowloris	5796
DoS Slowhttptest	5499
Bot	1966
Web Attack – Brute Force	1507
Web Attack – XSS	652
Infiltration	36
Web Attack – Sql Injection	21
Heartbleed	11

3.2 Veri Ön İşleme

Ön işleme aşamasında, veri setinde bulunan kayıtlardan sonsuz ya da anlamsız değerlere sahip olanlar tespit edilerek silinmiştir. Daha sonra herhangi bir değere sahip olmayan kayıtlar da çalışmada tutarlılığın sağlanması açısından silinmiştir. Son işlem olarak saldırının olup olmadığının belirlenebilmesi amacıyla kayıtların ikili sınıflandırmaya tabi tutulabilmesi için "Benign" etiketine sahip veriler "0", diğer tüm saldırı tipleri ise "1" olarak güncellenmiştir.

3.3. Öznitelik Seçimi

Özniteliklerin seçimi, üzerinde çalışılan örneği belirli kriterlere göre en iyi temsil edebilecek özniteliklerin mevcut öznitelik kümesi içerisinden seçilmesi işlemi iken, öznitelik çıkarılması ise yeni bir öznitelik uzayı oluşturmak amacıyla mevcut bilgilere dönüştürme işlemi uygulanmasıdır (Küçüksille ve Ateş 2016).

Çalışmada kullanılan veri setinde 83 farklı öznitelik bulunmaktadır. Oluşturulacak olan saldırı tespit sisteminde ağ trafiğinin izlenerek saldırı tespitinin başarı oranının artırılması ve çalışma zamanının da buna bağlı olarak mümkün olduğunca kısa tutulması amacıyla mevcut 83 farklı özniteliğin sayısının indirgenmesi gerekmektedir. Bu indirgeme işlemi sırasında sınıflandırma işleminde en başarılı sonuçları sağlayacak, sınıflandırma için en anlamlı özniteliklerin korunarak, sınıflandırma sürecinde

pek de etkisi olmayan özniteliklerin veri seti dışarısında bırakılmasına dikkat edilmiştir.

Saldırı tespitinde en anlamlı özniteliklerin seçilmesi adına çalışma boyunca farklı teknikler uygulanıp sonuçları değerlendirilmiştir. Öncelikle öznitelik seçim tekniklerinden biri olan Özyinelemeli Özellik Seçimi (RFE)(Recursive Feature Elemination) tekniği kullanılmıştır. Bu teknikte veri seti alt kümeler halinde istenilen bir denetimli öğrenme tekniği ile değerlendirilerek her alt kümenin en az değerli özelliği bulunarak küme dışına itilir ve bu işlem özyinelemeli olarak istenilen sayıda özellik kalana kadar devam eder (Int Kyn. 1). Çalışmada, Rastgele Orman (RF) denetimli öğrenme tekniği kullanılarak oluşturulan RFE modeli ile öznitelik sayısının 20'ye indirgenmesi sağlanmıştır.

Elde edilen 20 öznitelik ise İleri Yönelimli Seçim (Forward Selection)(FS) tekniği kullanılarak tekrar öznitelik seçim işlemine tabi tutulmuştur. Bu teknikte belirlenen bir p eşik değeri baz alınarak en başta boş küme olarak belirlenen özellikler kümesine adım adım özellik seçilir (Int Kyn. 2). Özelliklerin değerlerinin hesaplanmasında ise Sıradan En Küçük Kareler (Ordinary Least-Squares Model)(OLS) modeli kullanılır. Bu hesaplama tekniği ise bir veya daha fazla açıklayıcı değişken ile karesel hataların toplamını (buradaki hata kavramı sonuç değişkeninin tahmin edilen değeri ile gerçek değeri arasındaki farktır) en aza indiren sürekli veya en azından aralıklı sonuç değişkeni arasındaki ilişkiyi modeller (Zdaniuk 2014). Bu şekilde eşik değer altında kalan özellik kalmayana kadar adım adım devam eden işlemler sonucunda elde edilen özellikler veri setindeki en anlamlı öznitelikler olarak öne çıkar. Çalışmada bu yöntemle 20 öznitelik 16'ya düşürülmüştür.

Bunun dışında deney sayısını artırarak farklı öznitelik gruplarının seçilmesinin ortaya çıkacak sınıflandırma başarısına etkisini gözlemleyebilmek için makine öğrenmesi teknikleri haricinde manuel seçim yöntemiyle de belirli öznitelik grupları seçilerek sınıflandırma testlerine tabi tutulmuştur. Manuel öznitelik seçimlerinde literatürde bulunan çalışmalarda kullanılan öznitelikler, network bilgisine dayalı olarak daha fazla öne çıktığı düşünülen öznitelikler, ön çalışma sürecinde deneme-yanılma yoluyla elde edilen verilerde nispeten daha başarılı bulunan öznitelikler ve CICIDS 2017 veri seti üzerinde öznitelik önem dereceleri üzerinde yapılan çalışmalarda öne çıkan özniteliklerin kombinasyonuyla oluşan gruplar dikkate alınmıştır.

3.4. Sınıflandırma

Öznitelik çıkarma işleminden sonra veri setinden elde edilen özniteliklere göre veri setinde ön işlemden geçirilen kayıtlar sınıflandırılmıştır. Sınıflandırma işleminden önce veri setindeki kayıtların %80'i oluşturulacak olan modelin eğitimi için, %20'si ise modelin test edilmesi için ayrılmıştır.

Çalışmada sınıflayıcı olarak Naive Bayes (NB), Logistic Regression (LR), Decision Tree (DT), Random Forest (RF) ve Extreme Gradient Boosting (XGB) algoritmaları kullanılmıştır.

4. Bulgular

Deney sonuçlarının değerlendirilmesinde Karmaşıklık Matrisi (Confusion Matrix) ile Doğruluk (Accuracy), Kesinlik (Precision), Duyarlılık (Recall) ve F1 metriklerinden yararlanılmıştır. Karmaşıklık matrisinde TP(True Positive) doğru tahmin edilen pozitif verileri, TN(True Negative) doğru tahmin edilen negatif verileri, FP(False Pozitive) yanlış tahmin edilen pozitif değerleri ve FN(False Negative) ise yanlış tahmin edilen negatif değerleri temsil eder.

Doğruluk metriği (A), test aşamasında yapılan doğru tahminlerin sayısının toplam tahmin sayısına oranını ifade eder.

$$A = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

Kesinlik metriği (P), doğru tahmin edilen pozitif gözlem sayısının, pozitif olarak nitelendirilen tüm gözlem sayısına oranını gösterir.

$$P = \frac{TP}{TP+FP} \quad (2)$$

Duyarlılık metriği (R), doğru tahmin edilen pozitif veri sayısının gerçekte ne kadar pozitif veri olarak tahmin edilmesi gereken veri sayısına oranıdır.

$$R = \frac{TP}{TP+FN} \quad (3)$$

F1 metriği (F1 Score) ise Kesinlik ve Duyarlılık metriklerinin harmonik ortalamasını gösterir.

$$F1 = \frac{2xPxR}{P+R} \quad (4)$$

Çalışmada öncelikli olarak iki aşamalı seçimle elde edilen 16 adet özniteliğe (Paketlere ait ortalama varış zamanı, Paketin ortalama uzunluğu, İlk pencere içinde ileri yönde gönderilen byte sayısı, İleri yönde gönderilen paketlerin toplam uzunluğu, Geri yönde gözlenen ortalama segment boyutu, Paket uzunluk varyansı, İlk pencere içinde geri yönde gönderilen byte sayısı, Paketin standart sapması, Paketin maksimum uzunluğu, Ortalama paket boyutu, Geri yönde paketlerin maksimum uzunluğu, Hedef port, Geri yönde paketlerin standart sapması, Geri yönde alt akıştaki byte sayısı, Geri yöndeki paketlerin toplam uzunluğu, Geri yönde paketlerin ortalama uzunluğu) dayalı sınıflandırma işlemleri uygulanmıştır. Sınıflayıcılara göre elde edilen sonuçlar Çizelge 3 ve Çizelge 4'de gösterilmektedir.

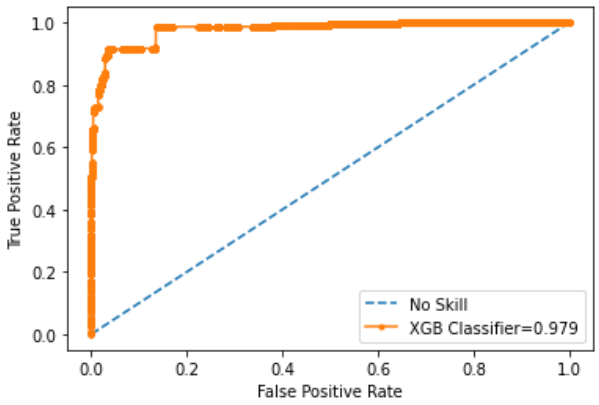
Çizelge 3. Birinci Sınıflandırmaya Ait Test Sonuçları

Sınıflayıcı	Doğruluk (Accuracy Score)	Kesinlik (Precision Score)	Duyarlılık (Recall Score)	F1 Score
XGB	0,93	0,93	0,93	0,92
NB	0,78	0,78	0,78	0,78
LR	0,89	0,89	0,89	0,88
DT	0,8	0,84	0,84	0,81
RF	0,94	0,93	0,93	0,93

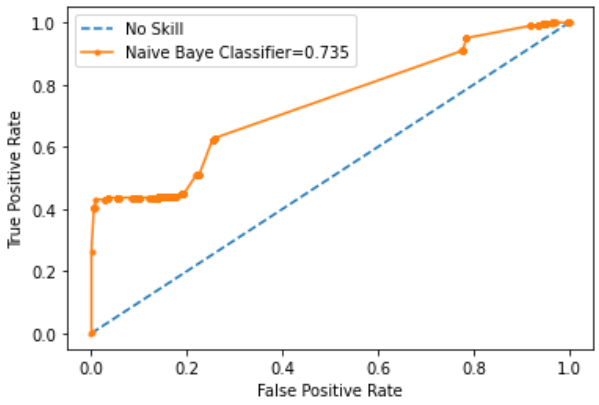
Çizelge 4. Birinci Sınıflandırmaya Doğrulama Sonuçları

Sınıflayıcı	Karmaşıklık Matrisi TP FP FN TN	Çapraz Doğrulama
XGB	453015 1113 40879 70569	0,99
NB	390178 63950 62695 48753	0,78
LR	447612 6516 53854 57594	0,89
DT	446331 7797 81089 30359	0,99
RF	447079 7049 31206 80242	0,98

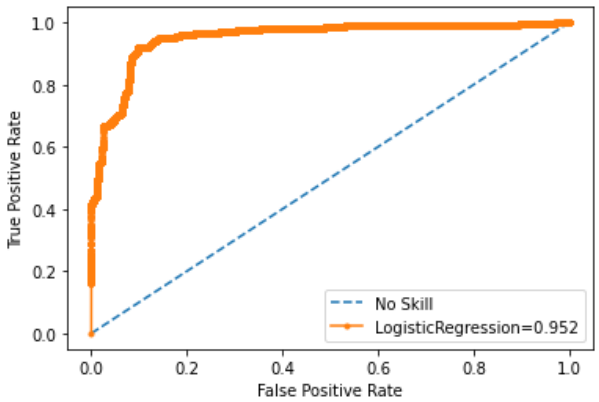
Birinci sınıflandırmada elde edilen verilere ait ROC eğrileri ise Şekil 1, Şekil 2, Şekil 3, Şekil 4 ve Şekil 5'te görülmektedir.



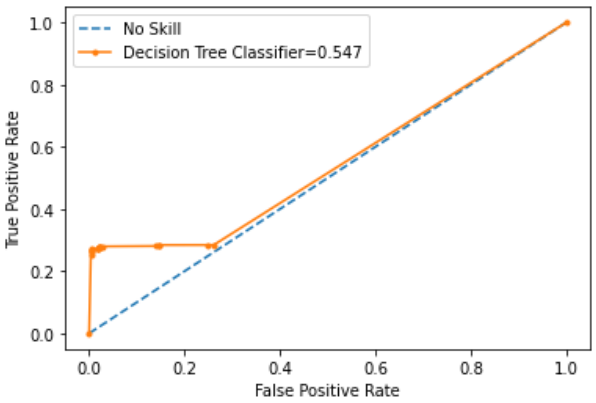
Şekil 1. Birinci Deneyde XGB Sınıflayıcısına Ait ROC Eğrisi



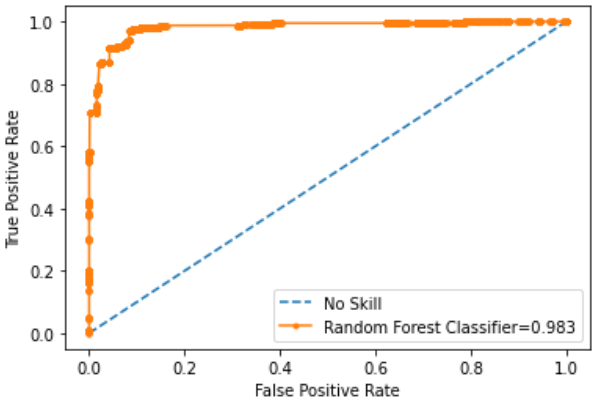
Şekil 2. Birinci Deneyde NB Sınıflayıcısına Ait ROC Eğrisi



Şekil 3. Birinci Deneyde LR Sınıflayıcısına Ait ROC Eğrisi



Şekil 4. Birinci Deneyde DT Sınıflayıcısına Ait ROC Eğrisi



Şekil 5. Birinci Deneyde RF Sınıflayıcısına Ait ROC Eğrisi

Bir diğer deneyde ise manuel olarak seçilen 14 adet özniteliğe (İleri yönde maksimum paket uzunluğu, İleri yönde paketlerin uzunluklarının standart sapması, Paketlerin en uzun varış zamanı, Paketlerin en kısa varış zamanı, Paketlerin ortalama varış zamanı, İleri yönde gönderilen iki paket arasındaki maksimum zaman, İleri yönde gönderilen iki paket arasındaki minimum zaman, İleri yönde gönderilen iki paket arasındaki ortalama zaman, Maksimum paket uzunluğu, Paket ortalama uzunluğu, Bir paketin uzunluk varyansı, İndirme/yükleme oranı, Ortalama paket boyutu, Paketin aktif hale gelmeden önce boşta kaldığı zaman) göre sınıflandırma işlemleri yapılmıştır. Sınıflandırma işlemlerine ait sonuçlar Çizelge 5 ve Çizelge 6'da gösterilmektedir.

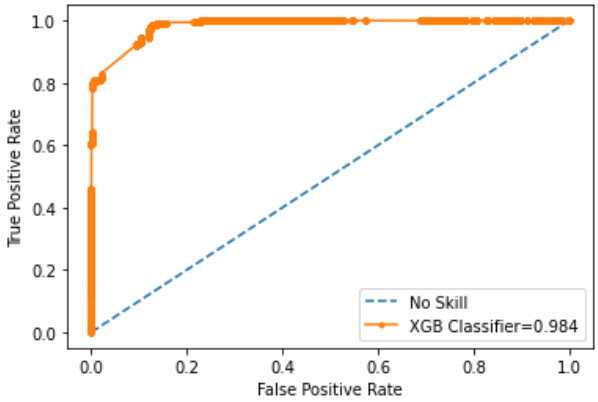
Çizelge 5. İkinci Sınıflandırmaya Ait Test Sonuçları

Sınıflayıcı	Doğruluk (Accuracy Score)	Kesinlik (Precision Score)	Duyarlılık (Recall Score)	F1 Score
XGB	0,92	0,93	0,92	0,91
NB	0,73	0,76	0,73	0,74
LR	0,88	0,89	0,89	0,87
DT	0,89	0,9	0,89	0,88
RF	0,92	0,93	0,92	0,92

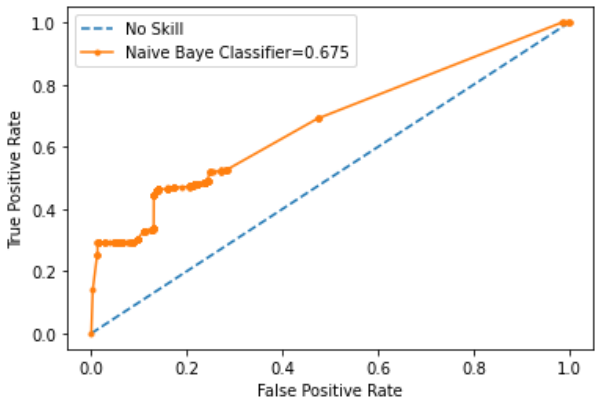
Çizelge 6. İkinci Sınıflandırmaya Ait Doğrulama Sonuçları

Sınıflayıcı	Karmaşıklık Matrisi TP FP FN TN	Çapraz Doğrulama
XGB	453986 142 43976 67472	0,98
NB	360981 93147 58405 53043	0,73
LR	451711 2417 61972 49476	0,88
DT	452974 1154 59895 51553	0,98
RF	453513 615 42855 68593	0,96

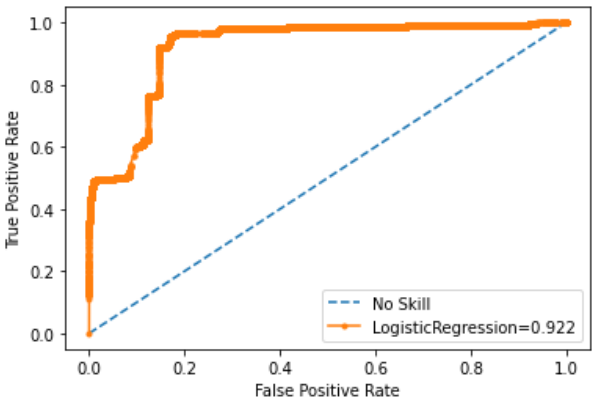
İkinci sınıflandırmada elde edilen verilere ait ROC eğrileri ise Şekil 6, Şekil 7, Şekil 8, Şekil 9 ve Şekil 10'da görülmektedir.



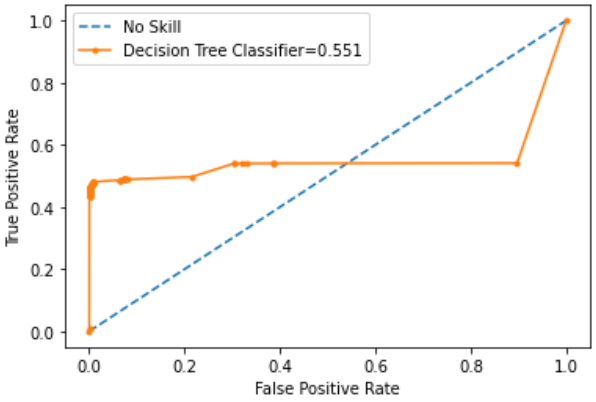
Şekil 6. İkinci Deneyde XGB Sınıflayıcısına Ait ROC Eğrisi



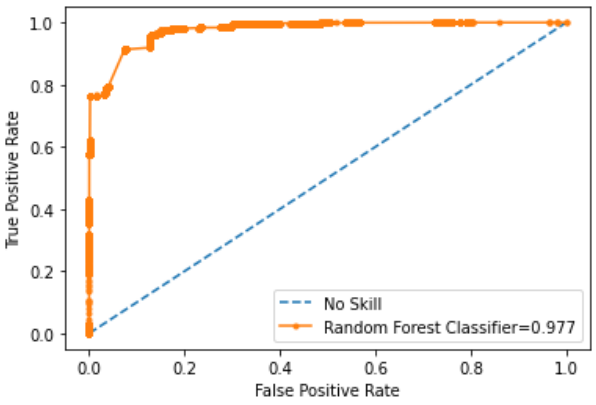
Şekil 7. İkinci Deneyde NB Sınıflayıcısına Ait ROC Eğrisi



Şekil 8. İkinci Deneyde LR Sınıflayıcısına Ait ROC Eğrisi



Şekil 9. İkinci Deneyde DT Sınıflayıcısına Ait ROC Eğrisi



Şekil 10. İkinci Deneyde RF Sınıflayıcısına Ait ROC Eğrisi

Son deneyde ise yine manuel olarak daha az sayıda öznitelik seçilmiştir. Seçilen 8 adet özniteliğe (Akış süresi mikrosaniye, Geri yöndeki paketlerin maksimum uzunluğu, Geri yöndeki paketlerin minimum uzunluğu, Geri yöndeki paketlerin ortalama uzunluğu, Minimum paket uzunluğu, PUSH bulunan paket sayısı, URG içeren paket sayısı, Geri yönde gözlenen ortalama segment boyutu) göre yapılan sınıflandırma işleminin sonuçları Çizelge 7 ve Çizelge 8'de verilmiştir.

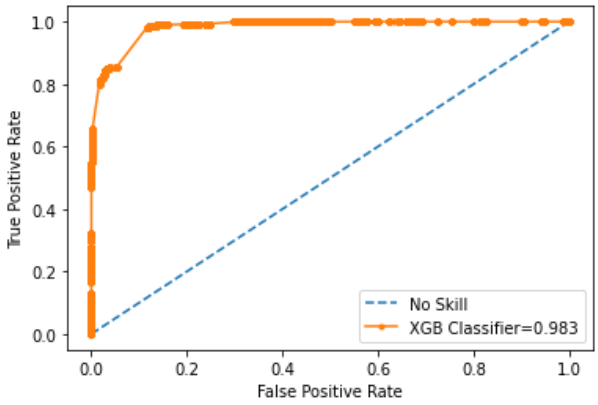
Çizelge 7. Üçüncü Sınıflandırmaya Ait Test Sonuçları

Sınıflayıcı	Doğruluk (Accuracy Score)	Kesinlik (Precision Score)	Duyarlılık (Recall Score)	F1 Score
XGB	0,93	0,93	0,93	0,92
NB	0,75	0,77	0,75	0,76
LR	0,88	0,88	0,88	0,86
DT	0,94	0,94	0,94	0,94
RF	0,93	0,93	0,93	0,93

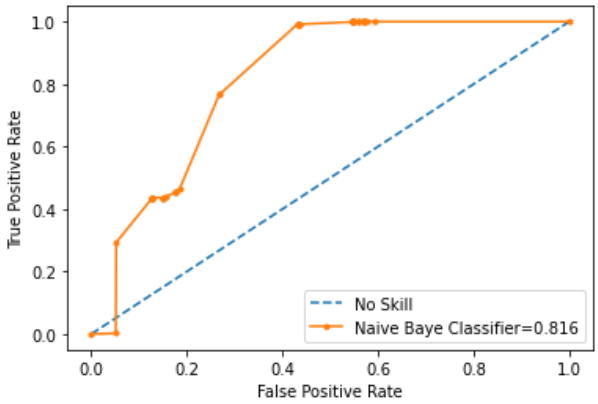
Çizelge 8. Üçüncü Sınıflandırmaya Ait Doğrulama Sonuçları

Sınıflayıcı	Karmaşıklık Matrisi TP FP FN TN	Çapraz Doğrulama
XGB	453514 614 40174 71274	0,96
NB	374540 79588 60954 50494	0,75
LR	447310 6818 62974 48474	0,87
DT	445940 8188 24747 86701	0,95
RF	446712 7416 31826 79622	0,93

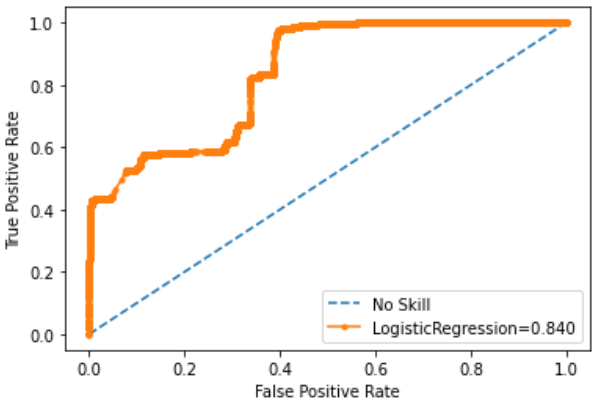
Üçüncü sınıflandırma deneyinde elde edilen verilere ait ROC eğrileri ise Şekil 11, Şekil 12, Şekil 13, Şekil 14 ve Şekil 15'te görülmektedir.



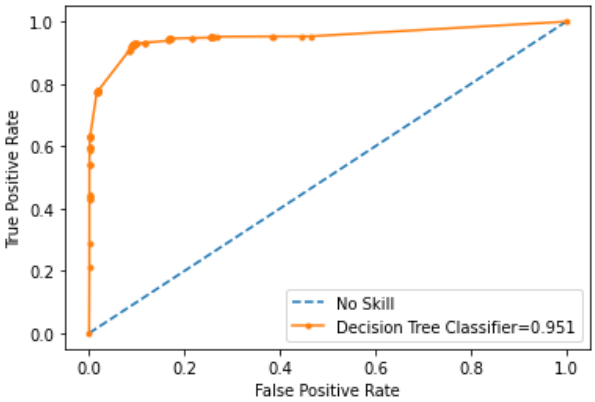
Şekil 11. Üçüncü Deneyde XGB Sınıflayıcısına Ait ROC Eğrisi



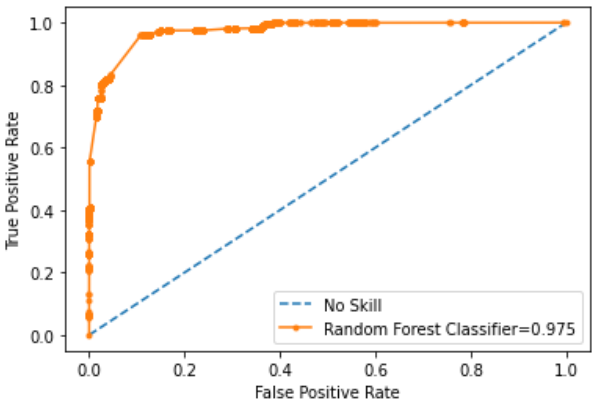
Şekil 12. Üçüncü Deneyde NB Sınıflayıcısına Ait ROC Eğrisi



Şekil 13. Üçüncü Deneyde LR Sınıflayıcısına Ait ROC Eğrisi



Şekil 14. Üçüncü Deneyde DT Sınıflayıcısına Ait ROC Eğrisi



Şekil 15. Üçüncü Deneyde RF Sınıflayıcısına Ait ROC Eğrisi

4.1. Farklı Öznitelik Gruplarıyla Yapılan Deney Sonuçlarının Tartışılması

Çalışma sürecinde elde edilen bulgular incelendiğinde hibrit yaklaşımla yapılan öznitelik seçimi sonrasında gerçekleştirilen sınıflandırma işlemlerinde Doğruluk metriğine göre en başarılı sonuç (0,94) RF sınıflayıcısı ile, Kesinlik, Duyarlılık ve F1 metriklerine göre en başarılı sonuçlar ise (0,93) hem RF hem de XGB sınıflayıcıları ile elde edilmiştir.

Çalışmada manuel olarak seçilen ilk öznitelik grubu ile gerçekleştirilen sınıflandırma sonuçlarına göre ise Doğruluk, Kesinlik ve Duyarlılık metriklerinde en başarılı sınıflayıcılar (0,93) XGB ve RF olurken, F1 metriğine göre ise en başarılı sonuçlar (0,92) RF sınıflayıcısı ile elde edilmiştir.

Çalışmanın manuel olarak seçilen son öznitelik grubu ile yapılan testlerde ise Doğruluk, Kesinlik, Duyarlılık ve F1 metriklerinin tamamında en başarılı sonuçlara (0,94) DT sınıflayıcısı ile ulaşılmıştır.

Oluşturulan modellerin ne kadar iyi çalıştığını görmek için ise Çapraz Doğrulama (Cross Validation) işlemi uygulanmış ve ROC eğrileri oluşturulmuştur. Deneylerde öne çıkan XGB, RF ve DT sınıflayıcıları ile oluşturulan modellerin Çapraz Doğrulama sonuçları incelendiğinde, bu sonuçların son derece başarılı olduğu gözlemlenmektedir.

ROC eğrisinde ise değişik eşik değerlerine göre yatay eksende yanlış pozitiflik (özgüllük) oranı bulunurken, dikey eksende ise doğru pozitiflik (duyarlılık) oranı yer alır. ROC eğrisi üzerindeki her nokta, farklı eşik değerlerine karşılık gelen duyarlılık ve özgüllük değerlerini ortaya koyar. Genelde düşük yanlış pozitiflik oranlarını veren eşik değerleri, düşük doğru pozitiflik oranına da sahiptir. Doğru pozitiflik oranı arttıkça, yanlış pozitiflik oranı da artar (Tomak ve Bek 2011). Deney sürecinde yapılan sınıflandırmalara ait ROC Eğrileri incelendiğinde ise XGB, LR ve RF sınıflayıcıları ile yapılan çalışmaların daha doğru sonuçlar verdiği görülmektedir.

Deneylere ait Çapraz Doğrulama ve ROC Eğrileri birlikte incelendiğinde ise XGB ve RF sınıflayıcılarının bahsedilen her iki analize göre de çok başarılı sonuçlar ortaya koyduğu görülmektedir. Bu da modellerin gösterdiği sınıflandırma sonuçlarının rastlantısal olarak değil gerçekten stabil bir modele göre tutarlı sonuçlar ortaya koyduğunu göstermektedir.

5. Sonuç

Bilgisayar ağlarına yönelik saldırıların önlenebilmesi, ilgili ağlarda ortaya çıkabilecek güvenlik zafiyetlerine

tedbir alınması ve daha çok kullanıcıların oluşturduğu güvenlik açıklarının kapatılmasıyla mümkün olabilmektedir. Bununla birlikte teknolojinin gelişimine paralel olarak artan kullanıcı sayıları ve uygulama çeşitliliği bu durumu zorlaştırmakta ve yapılan saldırı türlerini artırmaktadır. Sürekli gelişim ve değişim içinde olan bu konsept nedeniyle saldırı tespit ve önleme sistemleri de günden güne değişmekte ve gelişmektedir.

Yapılan bu çalışmayla ağlara yapılan saldırıların tespiti ve saldırı nedeniyle oluşabilecek her türlü zararın minimize edilebilmesi için ağ yönetimiyle ilgili ve yetkili kişilerin uyarılmasını sağlayacak olan bir karar destek modelinin oluşturulması üzerine bir araştırma yapılmıştır. Saldırı tespit sürecinde insan müdahalesinin olabildiğince az, makine öğrenmesi esaslarına dayanan ve ağ trafiğindeki olağan dışı hareketleri önceden tanımlanması gerek kalmadan yorumlayabilen bir sistem hedeflenmiştir.

Çalışma sonucunda elde edilen veriler ışığında saldırı tespitinde kullanılacak olan özniteliklerin en iyi şekilde seçilmesi gerektiği görülmüştür. Literatürdeki çalışmalar incelendiğinde öznitelik seçimi ve sınıflandırma aşamalarında benzer teknikler kullanıldığı görülse de bu çalışmada önerilen iki aşamalı hibrit öznitelik seçim yönteminin RF ve özellikle son yıllarda popüler olan XGB algoritmalarıyla birlikte saldırı tespitinde başarı oranını artırdığı anlaşılmaktadır. Daha çok deney tecrübesi ile manuel olarak seçilen daha az üyeye sahip öznitelik gruplarında ise DT algoritmasının bir miktar öne çıktığı görülse de hedeflenen modelde insan müdahalesinin minimize edilebilmesi için önerilen hibrit öznitelik seçim tekniği ve XGB, RF algoritmalarıyla yapılan saldırı tespitinin daha uygun olduğu tavsiye edilmektedir.

STS'lerde daha önce yapılan çalışmalarda kullanılan tekniklere nazaran hibrit öznitelik seçimi ve XGB algoritmasıyla yapılan sınıflandırma işleminin fark yarattığı düşünülmektedir. Çalışma sürecinde üzerinde çalışılan CICIDS2017 veri seti her ne kadar geniş ve kapsamlı olsa da gelecekte daha nitelikli dengeli şekilde oluşturulacak olan veri setleri üzerinde seçilen öznitelikler ve eğitilen modeller ile daha etkili sonuçlar alınacağı öngörülmektedir.

6. Kaynaklar

Abdel-Aziz, A.S., Hassanien, A.E., Azar, A.T. and Hanafi, S.E., 2013. Machine Learning Techniques for Anomalies Detection and Classification, *International Conference on Security of Information and Communication Networks*, 25-27 September, 2013, 219-229, Sydney-Australia.

Alamiedy, T.A., Anbar, M., Alqattan, Z.N.M. and Alzubi, Q.M., 2019. Anomaly-Based Intrusion Detection System Using Multi-Objective Grey Wolf Optimization Algorithm. *Journal of Ambient Intelligence and Humanized Computing*, **11**, 3735–3756.

Aljawarneh, S., Adlwairi, M. and Yassein, M.B., 2018. Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. *Journal of Computational Science,* **25**, 152–160.

Chen, W., Mei, F., Kong, F., Yuan, G. and Li, B., 2017. A Novel Unsupervised Anomaly Detection Approach for Intrusion Detection System. *2017 IEEE 3rd International Conference on Big Data Security on Cloud (Bigdata Security), High Performance and Smart Computing (HPSC) and Intelligent Data and Security (IDS)*, 26-28 May, 2017, 69-73, Beijing-China.

Fernandez, G.C. and Xu, S., 2019. A Case Study on Using Deep Learning for Network Intrusion Detection. *2019 IEEE Military Communications Conference (MILCOM)*, 12-14 November 2019, 1-6, Norfolk-VA-USA.

Jabez, J. and Muthukumar, B., 2015. Intrusion Detection System (IDS): Anomaly Detection using Outlier Detection Approach. *Procedia Computer Science,* **48**, 338-346.

Jose, S., Malathi, D., Reddy, B. and Jayasseeli, D., 2018. A Survey on Anomaly Based Host Intrusion Detection System, *National Conference on Mathematical Techniques and its Applications (NCMTA 18)*, 5-6 January 2018, 12-49, Kattankulathur-India.

Karataş, G. and Şahingöz, Ö.K., 2018. Neural Network Based Intrusion Detection Systems with Different Training Functions, *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, 22-25 March 2018, 1-6, Antalya-Türkiye.

Kumar, V., Choudhary, V., Sahrawat, V. and Kumar, V., 2020. Detecting Intrusions and Attacks in the Network Traffic using Anomaly based Techniques, *Proceedings*

of the Fifth International Conference on Communication and Electronics Systems (ICCES 2020), 10-12 June 2020, 554-560, Coimbatore-India.

Küçüksille, E.U. ve Ateş, N., Destek Vektör Makineleri ile Yaramaz Elektronik Postaların Filtrelenmesi. *Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi*, **6 (1)**, 2016.

Panigrahi, R. and Borah, S., 2018. A detailed analysis of CICIDS2017 dataset for designing Intrusion Detection Systems, *International Journal of Engineering & Technology*, **7**, 479-482.

Ran, J., Ji, Y. and Tang, B., 2019. A Semi-Supervised Learning Approach to IEEE 802.11 Network Anomaly Detection, *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*, 28 April – 1 May, 2019, 1-5, Kuala Lumpur-Malaysia.

Satam, P. and Hariri, S., 2020. WIDS: An Anomaly Based Intrusion Detection System for Wi-Fi (IEEE 802.11) Protocol, *IEEE Transactions on Network and Service Management*, **18(1)**, 1077-1091.

Shaukat, S., Ali, A., Batool, A., Alqahtani, F., Khan, J.S. and Ahmad, J., Intrusion Detection and Attack Classification Leveraging Machine Learning Technique, 14th International Conference on Innovations in Information Technology (IIT), Al Ain-United Arab Emirates, 198-202, 17-18 November, 2020.

Tomak, L. ve Bek, Y., 2021. İşlem Karakteristik Eğrisi Analizi ve Eğri Altında Kalan Alanların Karşılaştırılması. *Ondokuz Mayıs Üniversitesi Deneysel ve Klinik Tıp Dergisi*, **27 (2)**.

Yıldırım, M.Z., Çavuşoğlu, A., Şen, B. ve Budak, İ., 2014. Yapay Sinir Ağları ile Ağ Üzerinde Saldırı Tespiti ve Paralel Optimizasyonu. *XVI. Akademik Bilişim Konferansı Bildirileri,* 5-7 Şubat, 2014, 671-677, Mersin-Türkiye.

Zdaniuk, B., 2014. Ordinary Least-Squares (OLS) Model, Encyclopedia of Quality of Life and Well-Being Research, Editor: Michalos, A.C., Springer Netherlands, Dordrecth-Netherlands, 4515–4517.

Zhou, Y., Cheng, G., Jiang, S. and Dai, M., 2020. Building An Efficient Intrusion Detection System Based on Feature Selection and Ensemble Classifier, *Computer Networks*, **174**, 107247.

İnternet Kaynakları

1-https://scikit-learn.org/stable/modules/generated/sklearn.feature_selection.RFE.html, (18.02.2022)

2-https://www.analyticsvidhya.com/blog/2020/10/a-comprehensive-guide-to-feature-selection-using-wrapper-methods-in-python, (19.02.2022)