Avrupa Bilim ve Teknoloji Dergisi
Özel Sayı 32, S. 107-112, Aralık 2021

Araştırma Makalesi

www.ejosat.com ISSN:2148-2683

European Journal of Science and Technology
Special Issue 32, pp. 107-112, December 2021

Research Article

Saldırı Tespitinde Makine Öğrenmesi Yöntemlerinin Performans Analizi

Yasin Türkyilmaz[1], Arafat Şentürk[2*]

[1*] Düzce Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Düzce, Türkiye, (ORCID: 0000-0003-0150-9987), yasinturkyilmaz@duzce.edu.tr
[2] Düzce Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Düzce, Türkiye (ORCID: 0000-0002-9005-3565), arafatsenturk@duzce.edu.tr

(International Conference on Design, Research and Development (RDCONF) 2021 – 15-18 December 2021)

(**DOI:** 10.31590/ejosat.1045551)

ATIF/REFERENCE: Yasin, Türkyılmaz. & Arafat, Şentürk. (2021). Saldırı Tespitinde Makine Öğrenmesi Yöntemlerinin Performans Analizi. *Avrupa Bilim ve Teknoloji Dergisi*, (32), 107-112.

Öz

İnternete olan ilgi son yıllarda inanılmaz derecede artmış ve artmaya devam etmektedir. Bu artışa birde salgın hastalık koşulları eklenince insan hayatını etkileyen her şeyi internet vasıtasıyla yapmaya odaklanılmıştır. İnternete olan ilgi nasıl arttıysa bu ilgiyi suiistimal etmek isteyen kişilerde ve suç ifa edebilecek olan durumdaki faaliyetlerde de artmış ve istikrarlı şekilde artmaya devam etmiştir. Organizasyonların ağ güvenliğini sağlaması çok daha zor hale gelmiştir. Saldırı ve suçlulara karşı ağ güvenliğini sağlamak için birçok farklı güvenlik sistemleri kullanılmaktadır. Saldırı Tespit Sistemleri (STS) ağ güvenliği için kullanılan güvenlik sistemlerden bir tanesidir. STS aynı zamanda akademik dünyada da oldukça ilgi gören konudur. Son yıllarda araştırmacılar daha verimli ve etkin bir STS ortaya koymak için birçok çalışma yapmıştır. Yapılan çalışmalarda bencmark veri seti olarak kullanılan veri setlerinin günümüz şartlarını taşımadığı ve değerlendirmelerde doğru sonuçları vermediği görülmüştür. Bu soruna çözüm olması için 2015 yılında yayınlanan UNSW-NB15 veri seti oluşturulmuştur. Bu çalışmanın amacı STS'yi daha verimli ve etkin hale getirmek için kullanılan makine öğrenmesi yöntemlerinin UNSW-NB15 veri seti kullanılarak incelenmesi ve karşılaştırılmasıdır. Bunu yaparken kullanılan Özellik Seçim yönteminin algoritma performanslarına olan etkisi de değerlendirilmiştir. Çalışma kapsamında, Orange aracını kullanarak makine öğrenmesi yöntemlerinin performansları karşılaştırıldı. Ayrıca elde edilen sonuçlar ile daha önce yapılmış çalışmalar karşılaştırılmıştır.

Anahtar Kelimeler: Saldırı Tespit Sistemleri, Makine Öğrenmesi, UNSW-NB15.

Performance Analysis of Machine Learning Methods in Intrusion Detection

Abstract

Interest in the Internet has grown tremendously in recent years and continues to increase. When epidemic disease conditions are added to this increase, it is focused on doing everything that affects human life via the internet. Just as the interest in the Internet has increased, the number of people who want to abuse this interest has also increased in the number of attacks carried out over the Internet and in activities capable of committing crimes, and it has continued to increase steadily. It has become much more difficult for organizations to maintain network security. Many different security systems are used to provide network security against attacks and criminals. Intrusion Detection Systems (STS) is one of the security systems used for network security. STS is also a subject of great interest in the academic world. In recent years, researchers have done many studies to reveal a more efficient and effective STS. In the studies, it has been seen that the data sets used as the benchmark data set do not meet today's conditions and do not give the correct results in the evaluations. The UNSW-NB15 dataset, published in 2015, was created to solve this problem. The aim of this study is to examine and compare the machine learning methods used to make STS more efficient and effective using the UNSW-NB15 data set. Within the scope of the study, the performances of machine learning methods were compared using the Orange tool for the UNSW-NB15 dataset. In addition, performance evaluation was made with the results obtained and previous studies.

Keywords: Intrusion Detection System, Machine Learning, UNSW-NB15.

[*] Sorumlu Yazar: arafatsenturk@duzce.edu.tr

1. Giriş

İnternet, uygun internet protokolü (TCP/IP) kullanarak, cihazları küresel bir şekilde bağlayan bilgisayar ağlarının birbiriyle bağlı olduğu evrensel bir sistemdir (Sarkar, Chatterjee, and Misra 2018). İnternetin sağladığı en büyük avantaj bütün dünyanın bağlı olduğu ağ olma özelliğidir. Fakat bu özellik aynı zamanda güvenlik zafiyeti oluşturmaktadır. İnternet ağında var olan hiçbir veri gerekli önlemler alınmadığı takdirde güvende değildir. Bu duruma ek olarak internet ağı ile bağlantılı olan hiçbir ağ da gerekli güvenlik önlemleri alınmadığı taktirde güvenli sayılmaz (Fırlar n.d.).

İnternetin keşfinden sonra toplumların iletişim yapısı çok büyük bir değişime uğrayarak gelişmiştir. İki önemli güç olan iletişim ve bilişim, internet üzerinde buluşmuştur. Bu durum da kaçınılmaz olarak çok büyük ilgi görmüştür (Sarkar et al. 2018). Günümüzde iletişim ve haberleşme çok büyük oranda internet üzerinden gerçekleşmektedir. Sosyal medya, ana akım medyayı yakalamış ve neredeyse geçmiş vaziyettedir. Bu duruma ek olarak elektronik ticaret ve para transferleri gibi finansal konularda eklenince internet ağı üzerinden hizmet alan, veren veya internet ağına bir şekilde temas eden bütün ağlarda güvenlik tedbirlerinin alınması kaçınılmaz olmuştur.

Nesnelerin İnterneti (Nİ) gömülü cihazları, bilgisayarları ve algılayıcıları kablolu veya kablosuz ağ vasıtasıyla internete bağlayan bir iletişim ağıdır (Sarkar et al. 2018). Milyarlarca sayılara ulaşan Nİ cihazları izlenebilir ve kontrol edilebilirdir yapıya sahiptir. Cihazlar kendi aralarında iletişime veya etkileşime geçerek veri alışverişi yapabilirler. Nİ cihazlarını akıllı telefonlar, ev güvenliği (kamera) cihazları, akıllı televizyon vb. cihazlar olarak örneklendirilebilir (Chowdhury, Karmakar, and Kamruzzaman 2019). 1995 yılında dünya nüfusunun sadece %0.4 internete erişebilirken 2020 yılında bu oran %53' e ulaşmıştır (Anon n.d.).21.yy'da en önemli teknolojik gelişmeyi internetin sağladığı düşünülmektedir (Chowdhury et al. 2019).

İnternet teknolojisinin bu kadar büyümesinin olumsuz yönleri de ortaya çıkmıştır. Bunlardan en önemlileri arasında güvenlik problemleri vardır. Günümüzde, mahrem verileri saldırganlara karşı güvende tutmak gittikçe zorlaşan bir görev haline gelmektedir. Güvenlik önlemlerinin içerisinde geleneksel yöntemler olarak Güvenlik Duvarı, anti-virüs vb. yöntemler kullanmanın yanında artık yaşanan güvenlik sorunlarını en aza indirmek için farklı güvenlik yöntemleri de kullanılmaya başlamıştır. Bunlardan bir tanesi de Saldırı Tespit Sistemleridir. STS'ler iki farklı şekilde sınıflandırılmaktadır. Bunlar, İmza tabanlı STS'ler ve Anomali tabanlı STS'ler dir. İmza tabanlı STS'lerde önceden bilinen saldırılar vasıtasıyla karşılaşılacak herhangi bir saldırıyı önlemeyi amaçlamaktadır (Ata and Kadhim 2018). Önceden bilinen saldırıların imzaları oluşturulmuş ve bir veri tabanında saklanmaktadır. Ağ trafiğini tarayan STS'ler bu veri tabanındaki imzalar ile ağ trafiği karşılaştırılır ve eğer eşleşme meydana gelirse saldırı olarak nitelendirilir.

Bu yöntemde imza veri tabanı belli aralıklarla güncellenmesi gerekmektedir. Sıfır-gün saldırıları olarak bilinen saldırılara karşı yetersizdir (Moustafa and Slay 2016). Anomali bazlı STS'ler ise normal bir kullanıcı trafiğinin desenlerini MÖ yöntemleri yardımıyla belirleyerek bir model oluşturur ve bu modelin dışındaki herhangi bir ağ trafiğini anomali olarak nitelendirir. Bu yöntem sayesinde herhangi bir imza veri tabanı oluşturulması gerekmemektedir ve sıfır-gün saldırılarında oldukça başarılı sonuçlar elde edilmektedir (Moustafa and Slay 2016). MÖ yöntemleri Anomali tabanlı STS'lerin gelişmesinde çok önemli rol oynamaktadır.

Literatürde yapılmış çalışmalara dayanarak, bu çalışmada anomali tabanlı STS'lerin performanslarını etkileyen en önemli unsurlardan olan iki parametreyi ele alarak gerçekleştirildi.

Bunlardan birincisi, sağlıklı bir STS geliştirmek için eğitim verisini güncel ve günün şartlarını sağlamış olmasıdır. Bu konuda yapılan çalışmalarda benckmark veri seti olarak 1999 yılında oluşturulan ve sonraki yıllarda aynı veri seti üzerinde iyileştirmeler yaparak farklı veri setleri oluşturulduğu ve bu veri setlerinin kullanıldığı görülmüştür. 1999 yılında var olan saldırı tiplerinin günümüz şartlarını taşımadığı aşikardır (Kilincer, Ertam, and Sengur 2021). Literatürdeki yeni benckmark veri setleri üzerinden başarım analizlerinin yapılması gerektiği görüşüne katkı yapabilmek için, bu çalışmada literatürde yeni benckmark veri seti olarak kabul gören UNSW-NB15 veri setini kullanılmıştır.

İkincisi ise, saldırı tespiti yaparken kullanılan MÖ algoritmalarıdır. Çalışmada Orange aracı üzerinde denetimli MÖ algoritmalarını kullanılmıştır. Güncel bir veri seti ve o veri setine uygun MÖ algoritmalarının kullanarak sonuçlar alınmış. Ayrıca, veri setinin orijinal hali kullanılarakve veri seti üzerinde özellik mühendisliği uygulayarak tekrar sonuçlaralınmıştır. Daha sonar alınan tüm bu sonuçlar analiz edilmiş ve tartışılmıştır. Bu çalışmanın amacı STS'lerin çok daha verimli ve etkili çalışması için günümüz şartlarını taşıyan yeni bir bencmark veri seti kullanarak var olan MÖ yöntemlerinden hangisinin daha performanslı olduğuve kullanılan MÖ yöntemlerinin performanslarını karşılaştırmaktır.

2. İlgili Çalışmalar

Bu bölümde literatür araştırması yapılmış ve bu çalışmanın literature katkısından bahsedilmiştir.

Çetin Kaya ve ark.'nın gerçekleştirdikleri derleme çalışmalarında 2007-2013 yılları arasında alanıyla ilgili 65 çalışma incelemiş ve karşılaştırılmıştır. Bu incelemeler sonucunda araştırmacıların elde ettikleri sonuçlar sırayla şöyledir: STS'lerde en çok KDD Cup 99 veri setinin kullanılmıştır. DOS, Bilgi Tarama (proping), R2L, U2R gibi saldırı çeşitlerinin tespitinde Yapay Sinir Ağı (YSA) yüksek başarı göstermiştir. Destek Vektör Makineleri (DVM) ile DoS, Bilgi Tarama ve U2R tipi saldırılarda etkin çözümlerin üretilebileceğidir. Son olarakta, Bayes sınıflandırıcının Bilgi Tarama saldırılarında başarılı sonuçlar verdiğidir (Kaya and Yildiz 2014).

Liu Zhiqiang ve ark. UNSW-NB15 veri setini ve ileri beslemeli yapay sinir ağı algoritmasını kullanarak yeni bir ağ saldırı tespit sistemi modellemişlerdir. Veri seti seçimince KDD-Cup99 ve NSL-KDD gibi benckmark veri setlerinin aksine UNSW-NB15 veri setinin daha kullanışlı olduğunu belirtmişlerdir. Ek olarak, veri setinin normal ve saldırı ağ trafiğinin modern biçimde yansıttığı, yeni tip saldırıların güncelliğe sahip olduğunu ve sınıflandırma için çok uygun bir veri seti olduğunu belirtmişlerdir. Yapmış oldukları çalışmanın deneysel sonuçlarında ise yöntemlerden, Logistic Resression %83.15, Naive Bayes %81.2, Yapay Sinir Ağı %81.5 ve kendi önerdikleri yöntemin doğruluk oranı %99,9 olduğunu belirtmişlerdir (Zhiqiang et al. 2019).

Olamantanmi ve ark. 2020 yılında yaptıkları bir çalışmada gerçek zamanlı saldırı tespitine uygun bir yapay sinir ağ tabanlı STS geliştirmişlerdir. Geliştirilen STS'nin değerlendirilmesi için UNSW-NB15 veri seti kullanılmıştır. MÖ yöntemi olarak "Sinir Ağları" kullanılmıştır. Yapılan çalışmadan gerçek zamanlı ağ

trafiklerinde saldırı tespiti yaparken karşılaşılan zorluklarının en aza indirilmesi için özellik seçimi "gain oranı" yöntemi kullanılarak yapılmıştır. Orijinal haldeki veri setinde 49 olan özellik sayısı bu yöntemler kullanılarak 30'a düşürülmüştür. Deneysel sonuçlarda doğruluk oranının %76.96 olduğunu göstermiştir. Ayrıca sonuçlara dayanarak UNSW-NB15 veri setinin STS'lerin değerlendirilmesi için uygun bir veri seti olduğundan bahsetmişlerdir.(Mebawondu et al. 2020).

G. Kocher ve ark. 2020 yılında yapmış oldukları çalışmada UNSW-NB15 veri setini kullanarak MÖ yöntemlerinin sınıflandırma performanslarını karşılaştırmışlardır. Orijinal halinde 49 olan özellik sayısını MÖ yöntemlerinin sınıflandırma yaparken kullanılamayacak bazı özelliklerden oluşuyor olması sebebiyle bunları çıkartarak özellik sayısını 42'ye indirmişlerdir. Akış özellikleri olarak var olan özelliklerden 4 tanesi tek bir özelliğe indirilmiş ve zaman bildiren iki özellikte tek özelliğe indirgenmiş ve toplam özellik sayısı 45 olmuştur. Daha sonra id, dur ve attack_cat özellikleri listeden çıkarılmış ve toplam 42 özellikle uygulamalar yapılmıştır. Elde edilen sonuçlardan en yüksek doğruluk oranına "rassal orman" ile %95.43 olarak bulmuşlardır (Kocher and Kumar 2020).

Yapmış olduğumuz çalışma daha önce bu alanda yapılan çalışmalardan farklı olarak günümüz şartlarına uygun bir veri seti olan UNSW-NB15 veri setinde özellik sayısı relief yöntemi kullanılarak azaltılmışve bu veri setine uygun MÖ yöntemleri kullanarak performansları karşılaştırılmıştır. Çalışmamızda sadece veri setinin güncelliği değil aynı zamanda, bu veri setinde özellik mühendisliği uygulayarak elde edilen sonuçların iyileştirilmesini de içermektedir. Çalışmamızda MÖ yöntemlerini Orange aracı kullanarak uyguladık.

3. Materyal ve Metod

3.1. Saldırı Tespit Sistemleri (STS)

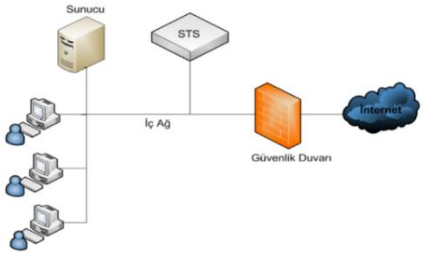
Saldırı Tespit Sistemleri (STS), hedef sistemin güvenliğinin sürdürülebilmesine olanak sağlamak için bilgisayar sistemlerindeki zararlı yazılımları tanımlayan yazılımsal veya donanımsal sistemlerdir (Liao et al. 2013). Karşılaşılan saldırılar, bilgi sistemlerinin yetkisiz kullanımına, değiştirilmesine veya tamamen ortadan kaldırılmasına sebep olarak bilgilerin gizlilik, bütünlük ve erişilebilirliğine yönelik tehdit oluşturur. STS bilgisayar güvenliğini sürdürmek için zararlı yazılım aktivitelerini tanımlamayı amaçlayan bir yapıdır (Khraisat et al. 2019).

Bilgisayar servislerinin meşru kullanıcıların isteklerine cevap veremeyecek hale getiren aktiviteler saldırı olarak düşünülmektedir. STS'nin hedefi geleneksel güvenlik duvarları tarafından tanımlanamayan ağ trafiğindeki farklı zararlı yazılım türlerinin tanımlanmaktır. Bunun yapılması bilgisayar sistemlerinin gizlilik, bütünlük ve erişilebilirliğini tehlikeye atan olaylar karşısında yüksek koruma sağladığı için hayati öneme sahiptir. STS'ler genel olarak iki gruba ayrılmaktadır: İmza Tabanlı STS (signature-based IDS) ve anomali tabanlı STS (anomaly-based IDS) (Khraisat et al. 2019). STS'lerin ağ topolojilerinde genelde Şekil 1'deki gibi konumlandırılmıştır.

3.2. Çalışmada Kullanılan Makine Öğrenmesi Algoritmaları

Makine Öğrenmesi, örnek veri veya deneyimlerden öğrenerek elde edilen performans kriterlerini en uygun durumuna getirmek için bilgisayarların programlanması bilimidir (Ata and Kadhim 2018). MÖ işlemlerinde, bilgisayarlar kendilerini besleyebilmek için eğitim veri seti olarak da bilinen veri örnekleriyle eğitilirler. Bilgisayarların öğrenim performansları test veri seti üzerinden test edilmektedir. MÖ genellikler klasik tekniklerin yetersiz olduğu durumlarda kullanılmaktadır (Ethem 2015).

Şekil 1. STS'lerin Ağ Topolojilerindeki Konumu



Bu çalışmasında, denetimli MÖ algoritmaları ele alınmış ve hedefin belirlenmesi için etiketli eğitim verisi kullanılmıştır. Etiketli veri ile eğitim aşaması tamamlandıktan sonra test veri seti ile performans ölçümleri yapılmıştır. Saldırı tespitinin belirlenmesinde kullanılan bu algoritmalar sırayla şunlardır;

- K-En Yakın Komşu (KNN)
- Rassal Orman (RO)
- Adaboost (AB)
- Lojistik Regresyon (LR)
- Naive Bayes (NB)
- Destek Vektör Makineleri (DVM)
- Sinir Ağları (SA)

3.3. UNSW-NB15 Veri Seti

Son yıllarda STS, var olan geleneksel güvenlik çözümlerinin yeterli olmadığı noktalarda MÖ yöntemlerini kullanarak başarılımı arttırmaktadır (Tsai et al. 2009). Özelliklede anomali bazlı STS'ler sıfır-gün atakları olarak bilinen saldırıların tespitinde çok önemli rol oynamaktadır. STS'lerin performanslarını değerlendirmek ve daha etkili ve verimli STS'ler oluşturmak için en önemli etkenlerden birisi kullanılan veri setleridir (Tsai et al. 2009). STS'lerin performanslarını ölçerken en çok kullanılan benchmark veri setleri; KDD99 ve NSLDKK'dir (Moustafa and Slay 2016). STS'lerin geliştirilmesi ve performanslarının ölçülmesinde veri setlerinin önemi çok büyüktür. Kullanılan veri seti çağın gereklerine uygun olmalı ve güncel saldırı tiplerini de barındırmalıdır. Literatürde en çok kullanılan KDD99 ve NSLKDD veri setlerinin atak tipleri çeşitliliğinde ve normal trafik senaryolarında çağımız şartlarından uzak olması, eğitim ve test veri setlerinin dağılımlarının farklı olması bu veri setlerinin olumsuz yönleri olarak karşımıza çıkmaktadır. Artık güncel veri setlerinin çalışmalarda kullanılması gerektiğini düşünmekteyiz. Bahsedilen bu sorunlara çözüm olması için son zamanlarda geliştirilen, güncel ve modern atak tiplerini içeren UNSW-NB15 veri seti ortaya çıkmıştır (Moustafa and Slay 2016).

UNSW-NB15 veri seti IXIA PerfectStorm aracı kullanılarak Avustralya siber güvenlik merkezi laboratuvarlarında hem gerçek modern normal aktivite hem de yapay günümüz şartlarına uygun ağ trafiği saldırı hareketlerini içeren hibrit bir model oluşturulmuştur. Tcpdump aracı ile 100 GB işlenmemiş ağ trafiğini yakalanmış ve ARgus ve Bro-IDS vb. araçlar 12 model veri setindeki özellikleri çıkarmak için geliştirilmiştir (Moustafa and Slay 2016).

Veri setinin geliştiricileri ayrıca veri setini eğitim veri seti ve test veri seti olarak iki farklı gruba da ayırmıştır. Bu veri seti

daha sonra birçok araştırmacı tarafından da kullanılmıştır (Moustafa and Slay 2016). Eğitim veri seti 175,341 kayıttan, test veri seti 82,332 kayıttan oluşmaktadır. Orijinal veri seti ise 2,540,044 kayıttan oluşmaktadır (Sonule et al. 2020). Eğirim ve test veri setinin saldırı sınıflarına göre dağılımları Tablo 1'de gösterilmiştir. Bu çalışmada veri seti olarak orijinal veri setinin geliştiricileri tarafından oluşturulan ve birçok araştırmacının da çalışmalarında kullandığı eğitim ve test veri seti olarak ikiye ayrılan alt örnek veri setini kullanılmıştır. Kullanılan veri setinde herhangi bir gereksiz kayıt içermemektedir.

Tablo 1. Saldırı Sınıflarına göre Veri Seti Dağılımı

Sınıf	Eğitim Seti	Test Seti
Normal	56,000	37,000
Analysis	2,000	677
Backdoor	1,746	583
DoS	12,264	4,089
Exploits	33,393	11,132
Fuzzers	18,184	6,062
Generic	40,000	18,871
Reconnaissance	10,491	3,496
Shellcode	1,133	378
Worms	130	44
Toplam Kayıt Sayısı	175,341	82,332

UNSW-NB15 veri seti toplam 49 özellik ve 1 hedef değere sahiptir. Çalışmada kullandığımız ve UNSW-NB15 veri setinden oluşturulan alt veri setinden 7 özellik çıkarılmıştır. Çıkarılan özellikler MÖ algoritmalarının kullanabileceği verileri içermediği için çıkartılmıştır. Örneğin, Kaynak IP adresi veya hedef port adresi vb. çıkarılan özelliklerden sonra özellik sayısı 42'ye düşmüştür.

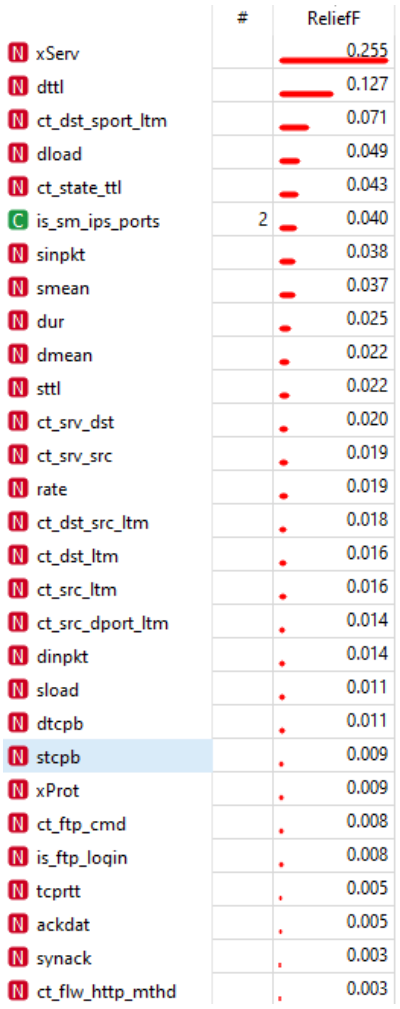
Çalışmamızda veri setinin 42 özelliğinin tamamının bulunduğu duruma normal veri seti olarak adlandırılmıştır. Literatürde puanlama yöntemi (scoring method) olarak bilinen ReliefF yöntemi kullanılarak orijinal veri setimizde 42 olan özellik sayısını azaltarak 29'a indilmiştir. Özellik sayısının azaltılmasında bütün özellikler içerisinden sınıflandırmada kullanılan özelliklerinsonuca etki değerlerine göre bir sıralama yapılmıştır ve en yüksek 29 özellik seçilmiştir. Seçilen bu özellikle Şekil 2'de Özellik sayısının azaltılmış olduğu veri setine ise özellik seçimi yapılmış veri seti olarak adlandırılmıştır.

3.4. Uygulama Araçları

3.4.1 Orange

Orange, Python ile yazılmış açık kaynak MÖ ve veri madenciliği aracıdır. Veriyi analiz edebilmek ve görselleştirmek için baştan sona görsel programlamaya sahiptir. Bu yazılım Ljubljana Üniversitesi bilgisayar fakültesi laboratuvarlarında geliştirilmiştir. Orange, veri madenciliği, veri analizi ve MÖ için bileşen tabanlı bir görselleştirme programıdır. Bileşenleri, öğrenme algoritmalarının ve tahmin modellemenin değerlendirilmesini yapabilmek için widget olarak adlandırılan ve veri görselleştirme, veri alt küme seçimi ve veri ön işleme aralığındaki widget'ları içinde barındırır. (Naik and Samant 2016)(Bisht et al. 2018). Yapılan çalışmanın benzetimi için seçilen Orange'ın ara yüzünün gelişmiş olması, MÖ algoritmalarının sınıflandırmada kullanımın kolay ve hızlı olması, verinin görselleştirilmesine olanak sağlaması tercih edilmede en önemli nedenlerindendir.

Şekil 2. ReliefF Yöntemi Sonrası Seçilen Özellikler



4. Araştırma Sonuçları ve Tartışma

4.1. Uygulama

Yapılan çalışmada özellik seçimi yapmaksızın orijinal veri ile kullanılan MÖ yöntemleriyle beş farklı kategoride performans değerlendirilmesi yapılmıştır. Özellik seçimi olmaksızın, eğitim veri seti ve test veri seti ayrı olarak kullanılmıştır. Elde edilen sonuçlar Tablo 2'de gösterilmiştir.

Tablo 2. Özellik seçimi yapılmadan MÖ algoritma performansları

MÖ Algoritması	Doğruluk	Hassasiyet	Duyarlılık	F-1 Skor
Rassal Orman	0.867	0.864	0.883	0.867
Sinir Ağları	0.856	0.852	0.872	0.856
Adaboost	0.856	0.851	0.876	0.856
K-En Yakın Komşu	0.783	0.773	0.808	0.783
Naive Bayes	0.751	0.751	0.766	0.751
Logistic Regresyon	0.706	0.676	0.765	0.706
DVM	0.449	0.297	0.474	0.449

ReliefF yöntemini kullanarak özellik seçimi yaptıktan sonra elde edilen yeni veri setini kullanarak doğrulama işlemi olarak

adlandırılan eğitim veri seti ve test veri setinin ayrı ayrı kullanılması sonucunda MÖ yöntemlerinin performanslarının sonuçları Tablo 3'de verilmiştir.

Tablo 3. Özellik Seçimi yapıldıktan sonra MÖ algoritma performansları

MÖ Yöntemi	Doğruluk	Hassasiyet	Duyarlılık	F-1 Skor
Rassal Orman	0.873	0.870	0.889	0.873
Adaboost	0.862	0.858	0.880	0.862
Sinir Ağları	0.948	0.856	0.877	0.862
K-En Yakın Komşu	0.783	0.774	0.808	0.783
Naive Bayes	0.751	0.751	0.766	0.751
Logistic Regresyon	0.706	0.676	0.765	0.706
DVM	0.449	0.297	0.474	0.449

5. Sonuç

5.1. Sonuçların Güncel Çalışmalar ile Karşılaştırılması

Olamantanmi ve ark. (Mebawondu et al. 2020) yapmış oldukları çalışmada UNSW-NB15 veri setini kullanmışlardır. Özellik seçimi yaparak MÖ algoritmalarından "sinir ağları" algoritmasını uygulamışlardır. Elde ettikleri sonuçlar ve bu çalışmada elde edilen sonuçlar Tablo 4'de verilmiştir.

Tablo 4. Çalışmamız ve Olamantanmi ve ark. çalışmasının karşılaştırılması

	Doğruluk (%)	Hassasiyet
Olamantanmi ve ark. (Mebawondu et al. 2020)	76.96	0.798
Önerilen Yöntem	85.6	0.852

G.Kocher ve G.Kumar (Kocher and Kumar 2020) 2020 yılında yapmış oldukları çalışmada UNSW-NB veri setini kullanarak MÖ algoritmalarının sınıflandırma performanslarını analiz etmişlerdir. Test veri setini oluştururken eğitim veri seti içerisinden belli oranda test veri seti oluşturulmuştur. Bağımsız bir test veri setleri bulunmamaktadır. Önerdiğimiz yöntemde ise test veri seti ve eğitim veri seti birbirlerinden bağımsız halde kullanılmıştır. Bu çalışmayı önerdiğimiz yöntem ile karşılaştırmanın sağlıklı yapılabilmesi için %20 oranında test işleminin yapılabilmesi gerekmektedir. Karşılaştırılan çalışmada herhangi bir özellik mühendisliği yapılmamış ve literatür kısmında belirttiğimiz gibi özellik sayısı orijinal veri setinde 49 iken 42'ye düşürülmüş ve uygulama yapılmıştır. Elde edilen sonuçlar ve önerdiğimiz yöntem ile elde edilen sonuçlar Tablo 5'de sunulmuştur. G. Kocher ve ark. ve önerdiğimiz çalışmanın MÖ yöntemlerinin performans analizleri Tablo 5'de verilmiştir.

Liu Zhiqiang ve ark. (Zhiqiang et al. 2019) yapmış oldukları çalışmada UNSW-NB15 ver setini kullanmışlardır. Yaptıkları çalışmada yeni bir Ağ STS modellemişlerdir. Çalışmalarının deneysel sonuçları ve önerdiğimiz yöntemin karşılaştırması Tablo 6'da gösterilmiştir.

Tablo 5. Önerilen yöntem ve G.Kocher ve ark. MÖ yöntemleri ile karşılaştırılması

	MÖ Yöntemi	Doğruluk	Hassasiyet	Recall	F1-Skoru
G. Kocher ve ark.	LR	93.23	0.92	0.99	0.95
Önerilen Yöntem		70.60	67.60	76.50	706
G. Kocher ve ark.	NB	48.03	1.00	0.23	0.38
Önerilen Yöntem		0.751	0.751	0.766	0.751
G. Kocher ve ark.	RO	95.43	0.96	0.97	0.97
Önerilen Yöntem		0.873	0.870	0.889	0.873
G. Kocher ve ark.	KNN	93.71	0.94	0.96	0.95
Önerilen Yöntem		0.783	0.774	0.808	0.783

Tablo 6. Çalışmamız ve L. Zhiqiang ve ark. çalışmasının karşılaştırılması

MÖ Yöntemi	Önerilen Yöntem	L. Zhiqiang ve ark. (Zhiqiang et al. 2019)
LR	0.706	0.8315
NB	0.751	0.812
SA	0.948	0.815

5.2. Sonuçların Değerlendirilmesi

Yapmış olduğumuz çalışma kendi içerisinde MÖ yöntemleri arasında karşılaştırılmıştır (Tablo 3). 172 bin kayıttan oluşan eğitim veri seti ile eğitilen denetimli MÖ algoritmalarını bağımsız bir veri seti olarak 82 bin kayıttan oluşan veri seti ile test edildi. Elde edilen sonuçlar göre en yüksek doğruluk oranına "Rassal Orman" algoritması olmuştur. Veri setinde bulunan 42 özellikten reliefF puanlama yöntemi kullanılarak 42 olan özellik sayısı 29'a indirgenmiş ve MÖ yöntemlerinin performasları tekrar analiz edilmiştir. Elde edilen sonuçlara göre özellik sayısının azalması elde edilen performans değerlerinde artışa sebep olmuştur. Özellik seçimi yaptıktan sonra da en yüksek doğruluk oranına sahip MÖ yöntemi "Sinir Ağları" olduğu görülmüştür. Bu çalışma literatür ile karşılaştırıldığında daha iyi sonuçlar elde ettiği görülmektedir.

Bu durumun başlıca sebebi özellik seçimi yaparken kullanılan reliefF yönteminin kullanılmasıdır. Literatürde de elde ettiğimiz bilgilere dayanarak özellikle Nİ cihazlarının heterojen bir yapıdan oluşması ve internet ağındaki kullanımının yoğunlaşması, güvenliği sağlamakta kullanılan MÖ algoritmalarının tek başlarına gösterdikleri performanslarının Topluluk Öğrenimi (TÖ) yöntemlerine nazaran daha düşük olduğudur.

İnternet gibi artık heterojen bir yapıya doğru giden ağ sistemlerinde saldırıların tespitinde TÖ yöntemlerinin performans analiz sonuçlarının daha yüksek çıkmasının nedeni

karşılaşılan her bir saldırı tipinin farklı MÖ algoritmalarının daha iyi tespit edilebildiğidir.

Gelecek çalışmalarda Birlitelik Kural Çıkarımı (BKÇ) ve Topluluk Öğrenimi (TÖ) gibi makine öğrenmesi yöntemlerinin kullanılarak sınıflandırmada çok daha yüksek doğruluk oranlarına ulaşılabileceği düşünülmektedir.

Kaynakça

Anon. n.d. "Statistics." Retrieved August 13, 2021 (https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx).

Ata, Oğuz, and Khalid Kadhim. 2018. "NETWORK INTRUSION DETECTION USING MACHINE LEARNING TECHNIQUES." *JOURNAL OF ENGINEERING SYSTEMS AND ARCHITECTURE Cilt* 2(1):115–23.

Bisht, Prithvi, Neeraj Negi, Preeti Mishra, and Pushpanjali Chauhan. 2018. "A Comparative Study on Various Data Mining Tools for Intrusion Detection." *International Journal of Scientific & Engineering Research* 9(5).

Chowdhury, Abdullahi, Gour Karmakar, and Joarder Kamruzzaman. 2019. "The Co-Evolution of Cloud and IoT Applications." 213–34. doi: 10.4018/978-1-5225-7335-7.CH011.

Ethem, Alpaydin; 2015. "Introduction to Machine Learning Second Edition Adaptive Computation and Machine Learning." *Massachusetts Institute of Technology* 41–470.

Fırlar, Talat. n.d. "AG GÜVENLİGi." SAU Fen Bilimleri Ensitüsü Dergisi 7. Cilt 1. Sayı, 2003

Kaya, Çetin, and Oktay Yildiz. 2014. "Makine Öğrenmesi Teknikleriyle Saldırı Tespiti: Karşılaştırmalı Analiz." *Marmara Fen Bilimleri Dergisi* 3:89–104. doi: 10.7240/mufbed.24684.

Khraisat, Ansam, Iqbal Gondal, Peter Vamplew, and Joarder Kamruzzaman. 2019. "Survey of Intrusion Detection Systems: Techniques, Datasets and Challenges." *Cybersecurity 2019 2:1* 2(1):1–22. doi: 10.1186/S42400-019-0038-7.

Kilincer, Ilhan Firat, Fatih Ertam, and Abdulkadir Sengur. 2021. "Machine Learning Methods for Cyber Security Intrusion Detection: Datasets and Comparative Study." *Computer Networks* 188:107840. doi: 10.1016/J.COMNET.2021.107840.

Kocher, Geeta, and Gulshan Kumar. 2020. "PERFORMANCE ANALYSIS OF MACHINE LEARNING CLASSIFIERS FOR INTRUSION DETECTION USING UNSW-NB15 DATASET." 31–40. doi: 10.5121/csit.2020.102004.

Liao, Hung Jen, Chun Hung Richard Lin, Ying Chih Lin, and Kuang Yuan Tung. 2013. "Intrusion Detection System: A Comprehensive Review." *Journal of Network and Computer Applications* 36(1):16–24. doi: 10.1016/J.JNCA.2012.09.004.

Mebawondu, J. Olamantanmi, Olufunso D. Alowolodu, Jacob O. Mebawondu, and Adebayo O. Adetunmbi. 2020. "Network Intrusion Detection System Using Supervised Learning Paradigm." *Scientific African* 9:e00497. doi: 10.1016/J.SCIAF.2020.E00497.

Moustafa, Nour, and Jill Slay. 2016. "The Evaluation of Network Anomaly Detection Systems: Statistical Analysis of the UNSW-NB15 Data Set and the Comparison with the KDD99 Data Set." *Http://Dx.Doi.Org/10.1080/19393555.2015.1125974* 25(1–3):18–31. doi: 10.1080/19393555.2015.1125974.

Naik, Amrita, and Lilavati Samant. 2016. "Correlation Review of Classification Algorithm Using Data Mining Tool: WEKA, Rapidminer, Tanagra, Orange and Knime." *Procedia Computer Science* 85:662–68. doi: 10.1016/J.PROCS.2016.05.251.

Sarkar, Subhadeep, Subarna Chatterjee, and Sudip Misra. 2018. "Assessment of the Suitability of Fog Computing in the Context of Internet of Things." *IEEE Transactions on Cloud Computing* 6(1):46–59. doi: 10.1109/TCC.2015.2485206.

Sonule, Avinashr, Mukesh Kalla, Amit Jain, and D. S. Chouhan. 2020. "Unsw-Nb15 Dataset and Machine Learning Based Intrusion Detection Systems." *International Journal of Engineering and Advanced Technology (IJEAT)* (9):2249–8958. doi: 10.35940/ijeat.C5809.029320.

Tsai, Chih Fong, Yu Feng Hsu, Chia Ying Lin, and Wei Yang Lin. 2009. "Intrusion Detection by Machine Learning: A Review." *Expert Systems with Applications* 36(10):11994–0.

Zhiqiang, Liu, Ghulam Mohi-Ud-Din, Li Bing, Luo Jianchao, Zhu Ye, and Lin Zhijun. 2019. "Modeling Network Intrusion Detection System Using Feed-Forward Neural Network Using UNSW-NB15 Dataset." *Proceedings of 2019 the 7th International Conference on Smart Energy Grid Engineering, SEGE 2019* 299–303. doi: 10.1109/SEGE.2019.8859773.