Avrupa Bilim ve Teknoloji Dergisi
Özel Sayı, S. 17-25, Ağustos 2020

Araştırma Makalesi

www.ejosat.com ISSN:2148-2683

European Journal of Science and Technology
Special Issue, pp. 17-25, August 2020

Research Article

Yapay Sinir Ağı Kullanılarak Anomali Tabanlı Saldırı Tespit Modeli Uygulaması

Mehmet Salih Karaman[1*], Metin Turan[2], Muhammed Ali Aydin[3]

[1] İstanbul Ticaret Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Bölümü, İstanbul, Türkiye ORCID: 0000-0001-9881-0666)
[2] İstanbul Ticaret Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, İstanbul, Türkiye (ORCID: 0000-0002-1941-6693)
[3] İstanbul Üniversitesi – Cerrahpaşa , Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, İstanbul, Türkiye (ORCID: 0000-0002-1846-6090)

(Bu yayın 26-27 Haziran 2020 tarihinde HORA-2020 kongresinde sözlü olarak sunulmuştur.)

(**DOI:** 10.31590/ejosat.778789)

ATIF/REFERENCE: Karaman, M. S., Turan, M. & Aydin, M. A. (2020). Yapay Sinir Ağı Kullanılarak Anomali Tabanlı Saldırı Tespit Modeli Uygulaması. *Avrupa Bilim ve Teknoloji Dergisi*, (Special Issue), 17-25.

Öz

Her geçen gün internetin yaygınlaşması ve buna bağlı olarak ağa bağlanan cihazların hızlı bir şekilde artması, bazı avantajlarının yanında birçok sorunu da beraberinde getirmektedir. Bu sorunlardan en önemlisi siber tehditlerdir. Kişilere, kurumlara ve devletlere karşı siber tehditler, maddi, itibar ve zaman gibi kayıplar verebilmektedir. Saldırı tespit ve saldırı önleme sistemleri, bu kayıpları ortadan kaldırmak veya en aza indirilebilmek için kullanılmaktadır. Saldırı tespit sistemleri imza tabanlı veya anomali tabanlı olarak tasarlanmakta ve günümüzde anomali tabanlı sistemler makine öğrenmesi yöntemleri kullanılarak geliştirilmektedir. Bu çalışmanın amacı, bir bilgisayar ağına saldırı olup olmadığını yüksek başarı oranı ile tespit etmenin yanı sıra, hangi saldırı türünün sisteme zarar vermeye çalıştığını da ayırt edebilen anomali tabanlı bir saldırı tespit sistemi tasarlamaktır. Bu sistemi geliştirmek için makine öğrenmesi yöntemlerinden olan yapay sinir ağları kullanılmıştır. Sistemin geçerliliğini sınamak üzere CSE-CIC-IDS2018 veri seti kullanılmıştır. Tehdit türleri olarak, yaygın sıklıkta karşılaşılan Botnet, DDOS, DOS, BruteForce saldırıları ele alınmıştır. Yapılan doğruluk sınamaları sonucunda, gelen bir paketin tehdit olup olmadığı %99.11 gibi çok yüksek bir başarım oranında doğru bulunmuştur. Ayrıca gelen tehdidin Botnet olduğu %93.23, DDOS olduğu %99.31, DOS olduğu %92.26 ve BruteForce olduğu %99.26 oranında doğru şekilde tespit edilmiştir.

Anahtar Kelimeler: Saldırı Tespit Sistemi, Siber Güvenlik, CSE-CIC-IDS2018 Veri Seti, Yapay Sinir Ağları

Model Application of Anomaly Based Intrusion Detection Using Artificial Neural Network

Abstract

The spread of the internet day by day and the rapid increase of the devices connected to the network, along with some advantages, brings together lots of problems.The most important one of these problems are cyber threats. Cyber threats towards individuals, institutions and states can cause losses such as material, reputation and time.Intrusion detection and intrusion prevention systems are used to eliminate these losses or to reduce attacks. Intrusion detection systems are being designed as signature-based or anomaly-based, and anomaly-based systems use machine learning methods. The purpose of these work is to develop an anomali-based system which determine with high success rate whether there is an attack on a computer network, as well as able to separate which type of attack tries to harm the system. Artificial neural networks, one of the methods of machine learning, were used to develop this system. CSE-CIC-IDS2018 data set were used to test the validity of the system. As type of threats, the common faced ones such as Botnet, DDOS, DOS, BruteForce attacks have been considered. As a result of the accuracy tests, it is found that whether an incoming package is a threat at a

[*] Sorumlu Yazar: İstanbul Ticaret Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Bölümü, İstanbul, Türkiye, (ORCID: 0000-0001-9881-0666), salih.krmn21@outlook.com

very high performance rate such as 99.11%. In addition, incoming threat was correctly determined 93.23% for Botnet, 99.31% for DDOS, 92.26% for DOS, and 99.26% for Brute Force.

Keywords: Intrusion Detection System, Cyber Security, CSE-CIC-IDS2018 Data Set, Artificial Neural Network

1 Giriş

Modern yaşam tarzının vazgeçilmezi haline gelen bilgi ve iletişim teknolojileri, ulusları bilgi ve iletişim alt yapılarına bağımlı hale getirmiştir. Günümüzde yaklaşık 2 milyar insan internet kullanmaktadır ve Microsoft'un araştırmasına göre bu sayının 2025 yılına kadar hızla artarak 4 milyarı geçmesi beklenmektedir (Yılmaz, Ulus, & Gönen, 2015). İnternetin geniş alanda kullanımı, bilgi teknolojisi olarak da adlandırılan "Siber Güvenlik" kavramını önemli hale getirmiştir.

'Stuxnet saldırısı' olarak da bilinen ve ABD tarafından 2009'da öne sürülen saldırının, İran'ın Natanz nükleer yakıt zenginleştirme tesislerine karşı düzenlendiğine inanılmaktadır (Çelik, 2013, s. 144). Yakın bir tarihte Gürcistan genelinde etkili olan siber saldırının; aralarında cumhurbaşkanlığının, sivil toplum kuruluşlarının, özel şirketlerin ve ulusal TV istasyonunun da bulunduğu 15 binden fazla web sitesini olumsuz etkilediği açıklanmıştır (SiberBülten, 2019) .

Karmaşık ve sürekli büyüyen ağ saldırılarına karşı en önemli savunma araçlarında biri Saldırı Tespit ve Önleme Sistemleri (STÖS)'dir. Bir Saldırı Tespit Sistemi (STS) ağı izleyerek güvenlik tehditlerini tespit etmeye çalışır ve sisteme bir saldırı tespit etmesi durumunda saldırı hakkında bilgi verir. Bu bilgi Saldırı Önleme Sistemleri (SÖS)'ne iletilir ve SÖS yöneticiye alarm gönderir ve kaynak adresin trafiğini engeller. Günümüzde birçok STÖS kullanılmaktadır. STS'lerin geliştirilmesinde, günümüze kadar istatistiksel yöntemler, kural tabanlı, eşik değeri belirleme, durum geçiş diyagramları, yapay sinir ağları, veri madenciliği, yapay bağışıklık sistemi, bulanık mantık gibi farklı birçok yaklaşım uygulanmıştır (Güven & Sağıroğlu, 2008).

STS'ler, imza tabanlı ve anomali tabanlı olmak üzere iki farklı şekilde tasarlanmaktadır. Bilinen saldırılar imza tabanlı STS'lerde bir veri tabanında tutulmaktadır ve gelen paketler bu veri tabanındaki verilerle kıyaslanarak saldırı olup olmadığı tespit edilmektedir. Ticari uygulamalarda çoğunlukla imza tabanlı STS'lerin kullanıldığı görülmektedir (Kalıpcıoğlu, Toğay, & Yolaçan, 2019). Anomali Tabanlı Saldırı Tespit Sistemleri (ATSTS) ise daha çok yapay zeka yöntemleri ile normal ve anormal veriler kullanılarak, sistemin eğitilmesi sonucu oluşturulurlar. Snort, Bro, Selks, Suricata, Ossec, Kfsensor, PhpIDS, .NetIDS, Firestorm yaygın olarak kullanılan STS'lerdendir (Baykara & Daş, 2019).

ATSTS daha önce karşılaşılmamış olan saldırılar karşısında iyi bir çözüm olarak görülmektedir. ATSTS'lerin modellenmesinde, istatistiksel temelli, önceden bilinen bilgilerin kullanılmasına dayanan veya örüntülerin sınıflandırılmasına dayanan yöntemler kullanılmaktadır (Garcı´a-Teodoroa, Dı´az-Verdejo, Macia´-Ferna´ndez, & Va´zquez, 2009).

Veri setleri içerisinde bir örneklem çok sayıda öz nitelik ile ifade edilebilmektedir. Çok fazla özellik kullanılarak tasarlanan bir modelin, en iyi performans göstereceğinin beklenmesi doğru değildir. Aksine bu durum, hesaplama maliyetini ve sistemin hata oranını arttırabilmektedir (Al-Jarrah, Siddiqui, Elsalamouny, Yoo, Muhaidat, & Kim, 2014). Bu yüzden bu çalışmada saldırı modelleri için farklı özellikler kullanılmıştır. Saldırının tespit edilme performansı değerlendirilerek, kullanılan özelliklerin en aza indirilmesi için BruteForce yöntemi kullanılmıştır.

Bu çalışmanın amacı, yaygın saldırılardan DDOS, DOS, BruteForce ve Bot 'un, normal ağ trafiğinden farklı özellikleri ile eğitilerek en yüksek başarımda bir ATSTS tasarlamaktır. Bu sisteminin geliştirilmesi, PyCharm IDE'si üzerinde Python programlama dili ve yapay sinir ağları öğrenme modeli kullanılarak yapılmıştır. Uygulamanın geçerliliğini sınamak üzere Kanada Siber Güvenlik Enstitüsü tarafından paylaşılan CSE-CIC-IDS2018 veri seti üzerinde sınanmıştır (CyberSecurity, 2018). Çalışma sonucunda gelen bir trafiğin tehdit olup olmadığı %99.11 oranında doğru tespit edilmiştir. Ayrıca gelen bir tehdidin Bot tehdidi olduğu %92.33, DDOS tehdidi olduğu %99.23, BruteForce tehdidi olduğu %99.33 ve DOS tehdidi olduğu %92.1 oranında doğru tahmin edilmiştir.

2 ATSTS ile İlgili Yapılmış Çalışmalar

ATSTS'lerin geliştirilmesinde, Yapay Sinir Ağları (YSA), k En Yakın Komşu, Naive Bayes, Destek Vektör Makineleri (DVM) gibi birçok makine öğrenmesi yöntemleri kullanılmıştır. Bu çalışmalar, yöntemler bazında ayrı ayrı aşağıda ele alınmıştır.

2.1 YSA Kullanılarak Yapılmış Çalışmalar

Kaynak kullanımını iyileştirmek ve zaman karmaşıklığını azaltmak üzere yapılan çalışmada, 41 öz nitelikli KDD-99 veri seti ve bu verinin 25 öz nitelikli hali, YSA kullanılarak test edilmiştir. Sonuçlar incelendiğinde, azaltılmış veri setinin saldırının olup olmadığımı tahmin yüzdesinin daha yüksek olduğu görülmüştür (AkashdeeP, Manzoor, & Kumar, 2017). KDD-99 veri seti üzerinde yapılan çalışmada Geri Beslemeli Sinir Ağı algoritması kullanılarak, saldırıları sınıflandıran bir STS tasarlanmıştır. Test sonuçları incelendiğinde, KDD-99 ile yapılmış diğer çalışmalara göre farklı saldırıları tespit etmede daha az sayıda yanlış pozitif ve yanlış negatif verdiği gözlemlenmiştir (Poojitha, Kumar, & Reddy, 2010). KDD-99 veri kümesindeki tüm özellikleri kullanılarak tasarlanan ATSTS'de YSA ve DVM performansı karşılaştırılmıştır. YSA'nın saldırı tespit doğruluğunun DVM'den daha iyi bir performansa sahip olduğu görülmüştür (Cahyo, Hidayat, & Adhipta, 2016).

2.2 k-en yakın komşu Algoritması Kullanılarak Yapılan Çalışmalar

NSL-KDD veri seti için TBA(Temel Bileşen Analizi / PCA) kullanılarak 6, 7, 11, 21 öz nitelik belirlenmiş, Naive Bayes , J-48, kNN-1 ve kNN-3 algoritmaları üzerinde 4 farklı veri seti kullanılarak, eğitim ve test işlemleri uygulanmıştır. Tehdit olup olmadığı,

%99,6871 doğruluk oranı ile TBA-21 veri setinde, kNN-1 algoritmasıyla elde edilmiştir. Fakat TBA-21 verisinin eğitim ve test süresi, diğer verilerin test ve eğitim sürelerine oranla oldukça yüksek çıktığı görülmektedir (Çavuşoğlu & Kaçar, 2019)

2.3 Naive Bayes Algoritması Kullanılarak Yapılan Çalışmalar

KDD-99 veri seti kullanılarak, DOS, R2L, U2R, Probing tehditlerinin tespitinde Naive Bayes ve Karar Ağacı tekniklerinin performansı test edilmiş ve test sonuçlarında Naive Bayes'in R2L ve Probing tehditleri için doğruluk oranının daha yüksek olduğu gözlemlenmiştir (Amor, Benferhat, & Elouedi, 2004). 41 özellikli NSL-KDD veri seti kullanılarak, öz nitelik sayısı 10, 14, 20, 24 olan veri setleri ve azaltılmamış veri setine Naive Bayes algoritması uygulanarak test edilmiştir. Test sonuçlarına göre, doğruluk oranı 24 öz nitelikli veri setinde en yüksek çıkmıştır. Tüm öz niteliklerin kullanılması ile elde edilen doğruluk oranı %95.11 iken, 24 öz nitelikli veri ile elde edilen doğruluk oranı %97.78'dir (Mukherjeea & Sharma, 2012).

2.4 Destek Vektör Makineleri Kullanılarak Yapılan Çalışmalar

DARPA veri seti kullanılarak, YSA ve DVM'nin bu veri seti üzerindeki performansının değerlendirildiği çalışmada, test sonucunda iki yöntemde de doğruluk oranı birbirine çok yakın çıkmıştır (%99'un üzerinde). Ama yeniden eğitimin yapılması gereken durumlar göz önüne alındığında, bu iki yöntemin eğitim süreleri: DVM 17.77 sn. YSA18 dk sürmüştür. Bu durum göz önüne alındığında DVM'nin performansının daha iyi olduğu değerlendirilmiştir (Mukkamala, Janoski, & Sung, 2002). NSL-KDD veri seti, TBA ile öz nitelik sayısı 41'den 23'e indirilmiştir. Öz niteliği azaltılmış veri seti ve azaltılmamış veri seti üzerinde, DVM kullanılarak yapılan deneylerde STS sisteminin, doğruluk oranlarının iki veri seti içinde birbirine çok yakın olduğu gözlemlenmiştir. Fakat azaltılmış veri setinin eğitim ve test süresi 2 kata yakın daha az sürede gerçekleştirdiği gözlemlenmiştir (Heba, Darwish, Hassanien, & Abraham, 2010).

3 Veri Seti ve Uygulama

3.1 Veri Seti

STS sistemlerinin iyileştirilmesi amacı ile birçok çalışma yapılmıştır. Bu çalışmaların çoğu, geçerli ve güncel bir veri seti bulunmadığından, mevcut birkaç veri seti üzerinde deneylerini gerçekleştirmişlerdir. DARPA, KDD'99, DEFCON, CDX, KYOTO, TWENTE, UMASS, ISCX bu veri setlerinden bazılarıdır (Sharafaldin, Arash, & Ali, 2018) .

Kanada Siber Güvenlik Enstitüsü tarafından paylaşılan, uygun bir test ortamında hazırlanmış CSE-CIC-IDS2018 veri seti, daha önce kullanılan veri setlerindeki eksiklikler dikkate alınarak oluşturulmuştur (CyberSecurity, 2018). Bu veri seti, 5 günlük bir test sürecinde tehdit yapıları ve iyi huylu davranış trafikleri göz önüne alınarak üretilmiştir. Veri seti PCAP dosya formatında üretilmiş, ağ trafiği akış üreteci olan CICFlowMeter uygulaması kullanılarak CSV formatına dönüştürülmüştür. Kanada Siber Güvenlik Enstitüsü tarafından paylaşılan bu veriler halkın kullanımına açılmış ve Siber Güvenlik alanında çalışma yapmak isteyen araştırmacılar bu veri setinin PCAP ve CSV formatına erişebilmektedir (CyberSecurity, 2018). Yapılan çalışmada bu veri seti kullanılmıştır.

3.1.1 Veri Setinin Özellikleri

Veri seti yerel bilgisayara indirilip incelendiğinde, içerisinde yer alan etiketler ve her bir etikete ait örnek sayısı Tablo1'de verilmiştir. Veri setinin PCAP formatı, CICFlowMeter aracılığıyla 79 özellikten ve 1 etiketten oluşan CSV formatlı dosyalara dönüştürülmüştür. Deney ortamında veri setinin test edilebilmesi için bazı ön işlemlerden geçmesi gerekmektedir. Ön işlemler için "string" veri türünden olan zaman parametresi sayısal değere dönüştürülmüştür. Ayrıca parametresi eksik olan verilerin olduğu tespit edilmiş ve bu örneklemler silinerek (normalleştirme) veri seti uygulama ortamı için uygun hale getirilmiştir.

3.1.2 Veri Seti Kullanılarak Yapılan Bazı Çalışmalar

Karar Ağacı ve Rastgele Orman Yöntemleri kullanılarak yapılan çalışmada, Hizmet Engelleme, Dağıtılmış Hizmet Reddi ve Port Tarama saldırıları anormal olarak etiketlenmiş ve deney sonuçlarında doğruluk oranı %99,966 ile Rastgele Orman daha başarılı sonuç vermiştir (Özekes & Karakoç, 2019). Her tehdidi belirleyen en iyi dört özelliğin bulunması amacıyla, K-en yakın komşu, Rassal Orman, ID3, Adaboost, çok katmanlı algılayıcı, Naive Bayes ve ikinci dereceden ayırım analizi yöntemleri kullanılmış, test ve eğitim süresi ve doğruluk değeri dikkate alındığında en iyi sonucu Rassal Orman yönteminin verdiği görülmüştür (Sharafaldin, Arash, & Ali, 2018).

3.2 Uygulama

Kolaylık sağlaması için her saldırı türüne ait dosyalar oluşturulmuş ve oluşturulan dosyalara saldırıya ait bilgiler yazılmıştır. Oluşturulan 13 farklı veri dosyası kullanılarak uygulama için 5 farklı veri seti oluşturulmuş ve bu veri setleri YSA ile eğitilmiştir.

1.veri seti herhangi bir tehdidin olup olmadığını kontrol etmek için oluşturulmuştur. Bu veri seti içerisinde normal olarak etiketlenen veriler Benign (zararsız) dosyasından alınmış ve Bot, BruteForce-Web, BruteForce-XSS, FTP-BruteForce, BruteForce-SSH, DDOS, Dos attacks Slowris, DoSattacks-GoldenEye, DoSattacks-Hulk, DoSattacks-SlowHTTPTest veri dosyalarından alınan veriler ise anormal durum olarak etiketlenmiştir. BruteForce denemeleri sonucunda 79 özellik içerisinden 17 özellik ile oluşturulan veri seti en iyi sonucu verdiği(%99,11) görülmüştür. Saldırı olup olmadığının tespitinde kullanılabilecek en iyi özellik kümesi ve açıklamaları Tablo 2'de verilmiştir.

Tablo 1 Veri Seti İçerisinde Yer Alan Etiketlere Ait Örneklem Sayıları

ETİKET	ÖRNEKLEM SAYISI
Benign (zararsız)	6000000
Bot	290000
BruteForce-Web	612
BruteForce-XSS	231
DDOS	690000
DoS attacks-Slowloris	11000
DoSattacks-GoldenEye	41500
DoSattacks-Hulk	462000
DoSattacks-SlowHTTPTest	140000
FTP-BruteForce	196000
Infilteration	161000
SQLInjection	90
SSH-Bruteforce	188000

Tablo 2 Saldırı Olup Olmadığının Tespiti için En İyi Özellik Kümesi ve Açıklamaları

ÖZELLİK	AÇIKLAMA
Flow Duration	Mikro-saniyedeki akış süresi
Flow Byts/s	Saniyede akan byte sayısı
Flow Pkts/s	Saniyede akan paket sayısı
Flow IAT Std	Paketlerin varış zamanlarının standart sapması
Flow IAT Max	Paketlerin maksimum varış Zamanı
Fwd IAT Tot	İleri yönde gönderilen iki paket arasındaki toplam zaman
Bwd Pkts/s	Saniyedeki geri yön paket Sayısı
Pkt Len Std	Bir akışın standart sapması
Pkt Len Var	Bir akışın uzunluk varyansı
RST Flag Cnt	RST içeren paket sayısı
ECE Flag Cnt	ECE içeren paket sayısı
Down/Up Ratio	İndirme ve yükleme oranı
Bwd Blk Rate Avg	Geri yönde kütle oranının ortalama sayısı
Init Fwd Win Byts	İleri yönde ilk pencere içinde gönderilen bayt sayısı
Fwd Act Data Pkts	İleri yönde en az 1 bayt TCP veri yüküne sahip paket sayısı
Fwd Seg Size Min	Geri yönde kütle oranının ortalama sayısı
Active Max	Boşta kalmadan önce bir akışın aktif olduğu maksimum zaman

2.veri seti tehdidin DDOS olup olmadığını kontrol etmek için oluşturulmuştur. Bu veri seti, zararsız durum için Benign veri dosyasından ve anormal durum için ise DDOS veri dosyasından alınarak oluşturulmuştur. Denemeler sonucunda 79 özellikten sadece 2 özellik ile en iyi sonucun (%99,31) elde edildiği görülmüştür. DDOS saldırı türü için belirlenen özellikler ve açıklamaları Tablo 3'te verilmiştir.

3.veri seti tehdidin BruteForce olup olmadığını kontrol etmek için oluşturulmuştur. Bu veri seti, zararsız durum için Benign veri dosyasından ve anormal durum için BruteForce-Web, BruteForce-XSS, FTP-BruteForce, SSH Bruteforce veri dosyalarından alınarak oluşturulmuştur. Denemeler sonucunda 79 özellikten sadece 6 özellik ile en iyi sonucun (%99,26) edildiği görülmüştür. BruteForce saldırı türü için belirlenen özellikler ve açıklamaları Tablo 4'te verilmiştir.

Tablo 3 DDOS Saldırısı Tespiti için En İyi Özellikler ve Açıklamaları

ÖZELLİK	AÇIKLAMA
Init Fwd Win Byts	İleri yönde ilk pencere içinde gönderilen bayt sayısı
Pkt Len Var	Bir akışın uzunluk varyansı

Tablo 4 Brute Force Saldırısı Tespiti için En İyi Özellikler ve Açıklamaları

ÖZELLİK	AÇIKLAMA
Flow Duration	Mikro-saniyedeki akış süresi
Bwd IAT Max	Geri yönde gönderilen iki paket arasındaki maksimum zaman
Flow Byts/s	Saniyede akan byte sayısı
Flow Pkts/s	Saniyede akan paket sayısı
Init Fwd Win Byts	İleri yönde ilk pencere içinde gönderilen bayt sayısı
Pkt Len Var	Bir akışın uzunluk varyansı

.

4.veri seti tehdidin Bot olup olmadığını kontrol etmek için oluşturulmuştur. Bu veri seti, zararsız durum için Benign veri dosyasından ve anormal durum için Bot veri dosyasından alınarak oluşturulmuştur. Denemeler sonucunda 79 özellikten sadece 4 özellik ile en iyi sonucun (93,23) elde edildiği görülmüştür. Bot saldırı türü için belirlenen özellikler ve açıklamaları Tablo 5'te verilmiştir.

Tablo 5 Bot Saldırısı Tespiti için En İyi Özellikler ve Açıklamaları

ÖZELLİK	AÇIKLAMA
Flow Byts/s	Saniyede akan byte sayısı
Flow Pkts/s	Saniyede akan paket sayısı
Pkt Len Var	Bir akışın uzunluk varyansı
Init Fwd Win Byts	İleri yönde ilk pencere içinde gönderilen bayt sayısı

5.veri seti tehdidin DOS olup olmadığını kontrol etmek için oluşturulmuştur. Bu veri seti, zararsız durum için Benign veri dosyasından ve anormal durum için DoS attacks-Slowloris, DoSattacks-GoldenEye, DoSattacks-Hulk, DoSattacks-SlowHTTPTest veri dosyalarından alınarak oluşturulmuştur. Denemeler sonucunda 79 özellikten sadece 6 özellik ile en iyi sonucun (%92,26) elde edildiği görülmüştür. DOS saldırı türü için belirlenen özellikler ve açıklamaları Tablo 6'da gösterilmiştir.

Tablo 6 DOS Saldırısı Tespiti için En İyi Özellikler ve Açıklamaları

ÖZELLİK	AÇIKLAMA
Flow Pkts/s	Saniyede akan paket sayısı
Pkt Len Var	Bir akışın uzunluk varyansı
Init Fwd Win Byts	İleri yönde ilk pencere içinde gönderilen bayt sayısı
Flow IAT Max	Paketlerin maksimum varış zamanı
Flow Duration	Mikro-saniyedeki akış süresi
Flow Byts/s	Saniyede akan byte sayısı

3.3 Sınıflandırıcıların Eğitilmesi ve Sınanması

Oluşturulan beş veri dosyasının içerisindeki verilerin %80'i eğitim %20 si sınama için ayrılmıştır. Her bir veri setine ait örneklem sayıları Tablo 7'de verilmiştir.

Tablo 7 Veri Setleri Eğitim ve Sınama Örneklem Sayısı

VERİ SETİ	EĞİTİM ÖRNEKLEM SAYISI	SINAMA ÖRNEKLEM SAYISI
1. Veri Seti	3.288.000	822.000
2. Veri Seti	1.096.000	281.000
3. Veri Seti	617.000	154.250
4. Veri Seti	460.800	115.000
5. Veri Seti	1.048.000	262.000

Eğitim PyCharm IDE'si üzerinde, Python dilindeki YSA algoritması kullanılarak yapılmıştır. Eğitimin gerçekleştirilmesi için Keras ve Scikit-learn kütüphanelerinden faydalanmıştır. Her bir sınıflandırıcının eğitilmesi esnasında geçen süre Tablo 8'de verilmiştir.

Tablo 8 Sınıflandırıcıların Eğitilmesi İçin Geçen Süre

VERİ SETİ	SINIFLANDIRICI TÜRÜ	EĞİTİM SÜRESİ
1. Veri Seti	Tehdit Olup Olmadığı	457 sn.
2. Veri Seti	DDOS	98 sn.
3. Veri Seti	BruteForce	123 sn.
4. Veri Seti	Bot	107 sn.
5. Veri Seti	DOS	552 sn.

Eğitimlerden sonra her bir sınıflandırıcı modeli test verilerinde sınanmak üzere saklanmıştır. Test verilerinde bu sınıflandırıcıların kullanılması sonucunda elde edilen doğruluk yüzdeleri Tablo9'da verilmiştir.

Tablo 9 Saldırı Türleri için Sınıflandırıcıların Doğruluk Yüzdeleri

TEST VERİSİ	SINIFLANDIRICI TÜRÜ	TEST SONUCU (%)
1. Veri Seti	Tehdit Olup Olmadığı	99,11
2. Veri Seti	DDOS	99,31
3. Veri Seti	BruteForce	99,26
4. Veri Seti	Bot	93,23
5. Veri Seti	DOS	92,26

4 Sonuç ve Gelecek Çalışmalar

Tablo 9'daki saldırı tespit başarım değerleri göz önüne alındığında, önerilen ATSTS modelinin saldırı tespiti ve özelleştirilmiş düzeyde en yaygın saldırı türleri olan Bot, BruteForce, DDOS ve DOS saldırılarının belirlenmesi amacı ile yüksek güvenirlilikte kullanılabileceğini göstermektedir. Önerilen ATSTS modelinin ayrıntılı akış şeması Şekil 1'de verilmiştir.

İlk aşamada CICFlowMeter, gelen trafik verisini ATSTS modelinin anlayacağı niteliklere dönüştürmek üzere kullanılmıştır. Daha sonra elde edilen 79 öz niteliğe sahip veriden, özellik azaltma uygulaması kullanılarak 5 farklı özellik kümesi oluşturulmuş ve bunlarla 5 adet farklı sınıflandırıcı oluşturulmuştur. İlk sınıflandırıcı 17 özellik ile eğitilmiş, tehdidin olup olmadığını sınamak üzere kullanılmaktadır. Eğer tehdit yoksa uygulamadan çıkılmaktadır. Tehdit varsa, tehdidin sınıfını bulmak üzere, farklı özellik kümeleri ile oluşturulmuş 4 farklı tehdit sınıflandırıcısı sırasıyla, tehdidin DDOS, Bot, BruteForce, DOS olup olmadığını kontrol etmektedir. Bu tehditlerin dışında bir tehdit oluştuğunda mevcut modelde sadece tehdidin olduğu bildirilmektedir.

Bu çalışma sonunda, önerilen ATSTS' nin ön uygulama olarak kullanılabileceğinin değerlendirilmesi için Tablo 10'da tehdidin var olup olmadığının tespiti, Tablo 11'de DDOS tehdidinin tespiti, Tablo 12'de BruteForce tehdidinin tespiti, Tablo 13'te Bot tehdidinin tespiti ve Tablo 14'te DOS tehdidin tespiti için yapılmış bazı çalışmalar ve bu çalışmaların test edilmesi sonucunda elde edilen doğruluk yüzdeleri verilmiştir. Tehdidin var olup olmadığı önerilen sistemde %99,11 oranında, DDOS tespiti %99.31 oranında, Brute Force tespiti %99.26 oranında, Bot tespiti %93.23 oranında, DOS tespiti %92.26 oranında doğru sonuçlar vermiş ve örnek çalışmalarla kıyaslandığında bütünleşik bir ATSTS olarak uygulanabilir olduğu görülmektedir. Önerilen sistemin, mevcut çalışmalara başarım olarak en uzak kalan tehdit tespitinin DOS saldırısı olduğu görülmektedir. Bununla birlikte elde edilen başarım oranı kabul edilebilir bir düzeydedir.

Bundan sonraki çalışmalarda derin öğrenme modelleri kullanılarak (örneğin CNN algoritması) başarım oranlarında daha iyi sonuçların mümkün olup olmadığı araştırılabilir. Ayrıca önerilen model, CSE-CIC-IDS2018 içerisindeki diğer saldırı türlerini de kullanabilecek biçimde çalışmanın kapsamı genişletilebilir.

Tablo 10 Birden Fazla Tehdidin Tespiti İçin Tasarlanan Bazı Çalışmalar

Yapılmış Çalışmalar	Kullanılan Veri Seti	Tehdit	Kullanılan Makine Öğrenmesi Yöntemi	Başarım Oranı (%)
(Özekes & Karakoç, 2019)	CSE-CIC-IDS2018	Port Tarama, DDOS, DOS	Rastgele Orman	99,96
(Sharafaldin, Arash, & Ali, 2018)	CSE-CIC-IDS2018	DDOS, DOS, BruteForce, Bot, SQL Injection, Infilteration	Rastgele Orman	98.00
(ATAY, ODABAŞ, & PEHLİVANOĞLU, 2019)	CSE-CIC-IDS2018	DDOS, DOS, BruteForce, Bot, SQL Injection, Infilteration	(CNN + Rastgele Orman)	98.05
(Basnet, Shash, Johnson, Walgren, & Doleck, 2019)	CSE-CIC-IDS2018	DDOS, DOS, BruteForce, Bot, SQL Injection, Infilteration	Derin Öğrenme	99,01

Tablo 11 DDOS Tehdidin Tespiti İçin Tasarlanan Bazı Çalışmalar

Yapılmış Çalışmalar	Kullanılan Veri Seti	Tehdit	Kullanılan Makine Öğrenmesi Yöntemi	Başarım Oranı (%)
(Kılınç, ve diğerleri, 2016)	YeZ ve NoZ	DDOS	Rastgele Orman	93,58
(Ll, E, Vélez, & O, 2016)	NSL-KDD	DDOS	Destek Vektör Makineleri	99.00

Tablo 12 BruteForce Tehdidin Tespiti İçin Tasarlanan Bazı Çalışmalar

Yapılmış Çalışmalar	Kullanılan Veri Seti	Tehdit	Kullanılan Makine Öğrenmesi Yöntemi	Başarım Oranı (%)
(Najafabadi, Khoshgoftaar, Kemp, Seliya, & Zuech, 2014)	SILK	Brute Force	Naive Bayes	99.75
(Najafabadi, Khoshgoftaar, Calvert, & Kemp, 2015)	NETFLOWS	Brute Force	C4.5N	99.65

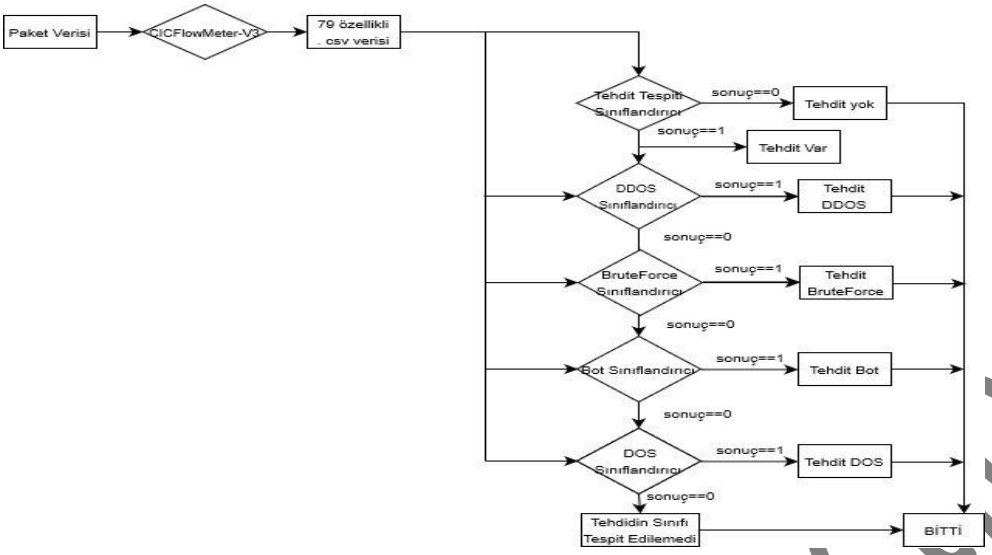
Tablo 13 Bot Tehdidin Tespiti İçin Tasarlanan Bazı Çalışmalar

Yapılmış Çalışmalar	Kullanılan Veri Seti	Tehdit	Kullanılan Makine Öğrenmesi Yöntemi	Başarım Oranı (%)
(Aydın, Sevi, & Salur)	Twitter	Bot	Lojistik Regresyon	79.1
(Tataroğlu, 2019)	Twitter	Bot	Derin Öğrenme	87..93
(Singh, Guntuku, Thakur, & Hota, 2014)	CAIDA and WireShark	Botnet	Rastgele Orman	99.98

Tablo 14 DOS Tehdidin Tespiti İçin Tasarlanan Bazı Çalışmalar

Yapılmış Çalışmalar	Kullanılan Veri Seti	Tehdit	Kullanılan Makine Öğrenmesi Yöntemi	Başarım Oranı (%)
(Kaya & Yıldız, 2014)	KDD cup99	DOS	Yapay Sinir Ağları	99.59
(Kaynar, Yüksek, Görmez, & Işık)	KDD cup99	DOS	Derin Öğrenme	99.42

Şekil 1 Önerilen ATSTS Modelinin Akış Şeması



Kaynakça

Çavuşoğlu, Ü., & Kaçar, S. (2019). Anormal Trafik Tespiti için Veri Madenciliği Algoritmalarının Performans Analizi. *dergipark* , 205-216.

Çelik, Ş. (2013). Stuxnet Saldırısı Ve Abd'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme. *Dergipark* , 144.

AkashdeeP, Manzoor, I., & Kumar, N. (2017). *A feature reduced intrusion detection system using ANN classifier.* ELSEVİER.

Al-Jarrah, O., Siddiqui, A., Elsalamouny, M., Yoo, P., Muhaidat, S., & Kim, K. (2014). Machine-Learning-Based Feature Selection Techniques for Large-Scale Network Intrusion Detection. *34th International Conference on Distributed Computing Systems Workshops.* Madrid: IEEE.

Amor, N. B., Benferhat, S., & Elouedi, Z. (2004). Naive Bayes vs decision trees in intrusion detection systems. *Proceedings of the 2004 ACM symposium on Applied computing* (s. 420-424). Nicosia: SAC.

Atay, R., Odabaş, D. E., & Pehlivanoğlu, M. K. (2019). İki Seviyeli Hibrit Makine Öğrenmesi Yöntemi İle Saldırı Tespiti. *Dergipark* , 258-272.

Aydın, İ., Sevi, M., & Salur, M. U. (Tarih Yok). Makine Öğrenmesi Algoritmaları İle Sahte Twitter Hesaplarının Tespiti.

Basnet, R. B., Shash, R., Johnson, C., Walgren, L., & Doleck, T. (2019). Towards Detecting And Classifying Network Intrusion Traffic Using Deep Learning Frameworks. . *Ournal Of Internet Services And Information Security (Jısıs)* , 1-17.

Baykara, M., & Daş, R. (2019). Saldırı Tespit Ve Engelleme Araçlarının İncelenmesi. *Dümf Mühendislik Dergisi* , 57-75.

Cahyo, A. N., Hidayat, R., & Adhipta, D. (2016). Performance Comparison Of İntrusion Detection System Based Anomaly Detection Using Artificial Neural Network And Support Vector Machine. *Aıp Conference Proceedings 1755.* Aıp.

Cybersecurity, C. I. (2018, 01 01). *Unb.Ca/Cic/Datasets/İds-2018*. 11 03, 2019 Tarihinde Unb.Ca: Https://Www.Unb.Ca/Cic/Datasets/İds-2018.Html Adresinden Alındı

Garcı´A-Teodoroa, P., Dı´Az-Verdejo, J., Macia´-Ferna´Ndez, G., & Va´Zquez, E. (2009). *Anomaly-Based Network İntrusion Detection:*. Elsevier.

Güven, E. N., & Sağıroğlu, Ş. (2008). Saldırı Tespit Sistemleri Üzerine Bir İnceleme. *3. Uluslararası Katılımlı Bilgi Güvenliği Ve Kriptoloji Konferansı* (S. 273-278). Ankara: Bildiriler Kitabı.

Gustavsson, V. (2019). Machine Learning For A Networkbased Intrusion Detection System. *Examensarbete Elektronık Och Datorteknık, Grundnıvå, 15 Hp* . Stockholm, İsveç: Kth Skolan För Elektroteknık Och Datavetenskap.

Heba, F. E., Darwish, A., Hassanien, A. E., & Abraham, A. (2010). Principle components analysis and Support Vector Machine based Intrusion Detection System. *Intelligent Systems Design and Applications (ISDA), International Conference on.* Cairo: IEEE.

Kılınç, D., Bozyiğit, F., Borandağ, E., Yücalar, F., Akyol, H., Akırmak, E. B., ve diğerleri. (2016). Sınıflandırma Tabanlı Zombi Bilgisayar Tespit Sistemi. *Akademik Bilişim 2016.* Aydın: Adnan Menderes.

Kalıpcıoğlu, K. C., Toğay, C., & Yolaçan, E. N. (2019). Son Kullanıcılar İçin Anomali Saldırı Tespit Sistemleri. *Eskişehir Osmangazi Üniversitesi Mühendislik Ve* , 199-212.

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

Kaynar, O., Yüksek, A. G., Görmez, Y., & Işık, Y. E. (Tarih Yok). Oto Kodlayıcı Tabanlı Derin Öğrenme Makinaları İle Saldırı Tespiti.

Kim, J., Shin, Y., & Choi, E. (2019). An Intrusion Detection Model based on a Convolutional Neural Network. *Journal of Multimedia Information System* , 165-172.

Ll, M. S., E, G. A., Vélez, J. I., & O, L. C. (2016). Distributed Denial of Service (DDoS) Attacks Detection Using Machine Learning Prototype. *In Distributed Computing and Artificial Intelligence, 13th International Conference* (s. 33-41). Cham: Springer.

Mukherjeea, D. S., & Sharma, N. (2012). *Intrusion Detection using Naive Bayes Classifier with Feature.* 120-128.

Mukkamala, S., Janoski, G., & Sung, A. (2002). Intrusion detection using neural networks and support vector machines. *Neural Networks (IJCNN), International Joint Conference on.* IEEE.

Najafabadi, M. M., Khoshgoftaar, T. M., Calvert, C., & Kemp, C. (2015). Detection of SSH Brute Force Attacks Using Aggregated Netflow Data. *2015 IEEE 14th International Conference on Machine Learning and Applications (ICMLA)* (s. 283-288). IEEE.

Najafabadi, M. M., Khoshgoftaar, T. M., Kemp, C., Seliya, N., & Zuech, R. (2014). Machine Learning for Detecting Brute Force Attacks at the Network Level. *2014 IEEE International Conference on Bioinformatics and Bioengineering* (s. 379-385). IEEE.

Ozekes, S., & Karakoç, E. N. (2019). Makine Öğrenmesi Yöntemleriyle Anormal Ağ Trafiğinin Tespit Edilmesi. *dergipark* , 566-576.

Poojitha, G., Kumar, K. N., & Reddy, P. J. (2010). Intrusion Detection using Artificial Neural Network. *2010 Second International conference on Computing, Communication and Networking Technologies.* Karur: IEEE.

Sharafaldin, I., Arash, H. L., & Ali, A. (2018). Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. *4th International Conference on Information Systems Security and Privacy (ICISSP).* Portekiz.

siberbulten.com. (2019, 10 29). 2 2020, 8 tarihinde siberbulten.com: https://siberbulten.com/siber-saldirilar-2/gurcistanda-siber-saldiri-15-bin-siteyi-vurdu-cumhurbaskanligi-dahil-bir-cok-kurum-etkilendi/ adresinden alındı

Singh, K., Guntuku, S. C., Thakur, A., & Hota, C. (2014). *Big data analytics framework for peer-to-peer botnet detection using random forests.* Information Sciences.

Tataroğlu, V. (2019). *Derin öğrenmeye dayalı sosyal medya profillemesi.* Denizli: Pamukkale Üniversitesi Fen Bilimleri Enstitüsü.

V.Kanimozhi, & PremJacob, T. (2019). Artificial Intelligence based Network Intrusion Detection with hyper-parameter optimization tuning on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing. *ICT* , 211-214.

Yılmaz, E., Ulus, H., & Gönen, S. (2015). Bilgi Toplumuna Geçiş Ve Siber Güvenlik. *Dergipark* .