DÜMF Mühendislik Dergisi
web: http://dergipark.gov.tr/dumf

Araştırma Makalesi / Research Article

Filtreleme Tabanlı Öznitelik Seçme Yöntemlerinin Anomali Tabanlı Ağ Saldırısı Tespit Sistemlerine Etkisi

Ömer EMHAN*
Dicle Üniversitesi, Elektrik Elektronik Mühendisliği Bölümü, Diyarbakır
oemhan@dicle.edu.tr ORCID: 0000-0003-0053-622X

Mehmet AKIN
Dicle Üniversitesi, Elektrik Elektronik Mühendisliği Bölümü, Diyarbakır
makin@dicle.edu.tr ORCID: 0000-0001-5439-4824

Geliş: 15.05.2019, Kabul Tarihi: 31.05.2019

Öz

Ağ akış verileri, büyük boyutlu verilerdir ve makine öğrenmesi algoritmaları ile tüm verinin işlenerek anomali tespitinin yapılmasını zorlaştırmaktadır. Ancak, ağ akış verilerini sınıflandırmak için tüm öznitelikler gerekli değildir. Gereksiz öznitelikler işlem yükünü arttırırken, aynı zamanda tespit oranlarını da azaltır. ÖS, veri setini temsil edebilecek en iyi öznitelikleri belirlemeye yarar. Bu bilgiler kapsamında bu çalışmada, filtreleme tabanlı öznitelik seçme (ÖS) yöntemlerinin internet ağlarında anomali tabanlı saldırı tespit sistemlerine (STS) etkisinin araştırılması amaçlanmıştır. Çalışmada NSLKDD veri kümesi kullanılmıştır. NSLKDD veri kümesindeki KDDTrain20Percent veri kümesi eğitim için, KDDTest veri kümesi test için kullanılmıştır. Böylece farklı bir veri kümesi ile eğitilen sistem farklı bir test kümesi ile test edilerek sistemin güvenilirliği ispatlanmıştır. Veri kümesinde 41 adet öznitelik yer almaktadır. Çalışmada ilk olarak filtreleme tabanlı Bilgi Kazancı, Kazanç Oranı, Simetrik Belirsizlik Katsayısı, Ki-Kare, One-R ve Korelasyon Tabanlı Öznitelik Seçimi yöntemleri ile veri boyutu azaltılmıştır. Her bir öznitelik seçme yönteminde sıralama usulüne göre ilk 8 öznitelik seçilip son veri kümesi olarak sınıflandırıcılara sürülmüştür. Öznitelik vektörleri k-En Yakın Komşuluk (k Nearest Neighnorhood-KNN) ve Rastgele Orman (RO) yöntemleri ile sınıflandırılmıştır. Performans ölçütleri olarak; işlem süresi, doğruluk, pozitif doğru oranı, pozitif yanlış oranı ve ROC (Receiver Operator Characteristic) eğrisi altındaki alan değerleri kullanılmıştır. Sınıflandırıcı açısından, RO yönteminin gerek ham veri kümesi, gerekse 8 özniteliğe indirgenmiş veri kümeleriyle elde edilen sonuçlarının KNN yöntemine göre daha başarılı olduğu görülmüştür. Tüm sonuçlar değerlendirilince Bilgi Kazancı, Ki-Kare, One-R yöntemleri ile elde seçilen özniteliklerin RO yöntemi ile sınıflandırılmasının en optimum yöntem olduğu gözlemlenmiş olup ÖS yöntemlerinin STS 'lere olumlu yönde katkı sağladığı sonucuna varılmıştır.

Anahtar Kelimeler: *Ağ Saldırı Tespiti; Filtreleme tabanlı öznitelik seçimi*

* Yazışmaların yapılacağı yazar

DOI: 10.24012/dumf.565842

Giriş

Dünya üzerindeki ilk bilgisayarlar arası ağ yapısı 1969'da kurulan Arpanet (Advanced Research Projects Agency Network) ağ yapısıdır ve temel görevi, bağlı olan birkaç üniversitenin ana bilgisayarları arasındaki iletişimin sağlanmasıdır. Böylece farklı fiziksel mekânlardaki bilimsel araştırmacıların bir birleri ile ağ üzerinden dosya paylaşımında bulunmaları imkânlı hale gelmiştir. Ağ teknolojisinin günümüzdeki gibi yaygın kullanılacağı tahmin edilememiş, sistemin güvenliği pek önemsenmemiştir. Ancak bilişim teknolojileri kullanımı hayal edilenin çok ötesinde bir noktaya gelmiş olup bu sistemin güvenliği kritik bir öneme sahip hale gelmiştir. Bilişim teknolojilerinin kullanımı artmasıyla birlikte kötüye kullanım da aynı şekilde artmıştır.

Bilgi güvenliği bilginin gizliliği, güvenilirliği ve hizmetin sürekliliği esas alınarak değerlendirilir. Siber ortamda bilgi güvenliği kimlik doğrulama, anti virüs yazılımları, güvenlik duvarları, saldırı önleme sistemleri gibi mekanizmaların yalnız veya bir arada kullanılmasıyla sağlanmaktadır. Bu tip güvenlik sistemlerinin koruma yeteneği veri tabanlarının güncelliği ölçüsündedir. Veri tabanlarının önceden hiç görmediği sıfırıncı gün saldırıları olarak isimlendirilen saldırıların önlenmesi kural tabanlı sistemlerden ziyade, sistemin hareketlerinin sürekli izlenmesi ve anormal durumların tespit edilmesi ile mümkündür. Bu durum ağ güvenliğini bir sınıflandırma problemine dönüştürür. (Nour M., Jiankun H., Jill S., 2019)

Ağ verileri, büyük boyutlu verilerdir ve makine öğrenmesi algoritmaları ile tüm verinin işlenerek anomali tespitinin yapılmasını zorlaştırmaktadır. STS 'ler pek çok öznitelik içeren büyük miktardaki bu ağ verilerini işler. Ancak, ağ akış verilerini sınıflandırmak için tüm öznitelikler gerekli değildir. Gereksiz öznitelikler işlem yükünü arttırırken, aynı zamanda tespit oranlarını da azaltır. Öznitelik seçimi (ÖS), ağ akış verilerinin tüm özniteliklerinden yalnızca önemli olanları veya belirlenenleri bulmak için kullanılır. Bu sebepten STS 'lerde ağ akış verilerinden değerli özniteliklerin seçimi önemli bir konudur (Lee et al. 2012). ÖS yöntemleri genel olarak sarmal yöntemler ve filtreleme tabanlı yöntemler olarak 2 kısımda incelenir. Bu çalışmada 6 farklı filtreleme tabanlı ÖS yöntemi ile veri indirgenmiş ve bu işlemin sistemin başarımına etkisi araştırılmıştır. Elde edilen sonuçlara göre bazı veri indirgeme yöntemleri, sistemin başarımını az miktarda düşürmüş olsa da veri boyutunun azalmasından dolayı işlem yükünü azaltmış ve işlem süresini kısaltmıştır. Öte yandan bazı veri indirgeme yöntemleri işlem süresini kısaltmakla birlikte sistemin başarımını da arttırmıştır ki bu umut verici bir sonuçtur.

Literatürde ÖS yöntemleriyle yapılan birçok çalışma mevcuttur. Çalışmamızda kullandığımız filtreleme tabanlı ÖS yöntemleri kullanılarak yapılan bazı çalışmalar özetlenmiştir.
Alazab ve ark. (2012) NSL-KDD verilerine bir filtreleme tabanlı ÖS tekniği olan *Bilgi Kazancı* uyguladılar ve toplam öznitelik sayısını 41'den 12'ye düşürdüler. Sınıflandırıcı olarak *Karar Ağacı* kullandılar. Özniteliklerin azaltılması sonrasında modelin 5 kat daha hızlı sonuç verdiğini tespit ettiler. Ayrıca, sınıflandırma doğruluğu olarak, ROC eğrisi altındaki alan değerleri için 5 farklı saldırı sınıfının ağırlıklı performans ortalaması göz önüne alındığında sonucun hafifçe iyileştiğini gözlemlediler.
Li ve ark. (2006), KDD 99 veri setindeki öznitelik sayısını *Bilgi Kazancı* ve *Ki-Kare* teknikleri kullanarak 41'den 6'ya düşürdüler. Her iki tekniğin de aynı en iyi 6 özniteliği sağladığını gözlemlediler. Bu ilk 6 öznitelik her teknik için farklı olarak sıralanırken, her iki teknikte de ilk 6 öznitelik dışındaki özniteliklerin "değerlilik" ölçütünde çok önemli düşüşler olduğunu tespit ettiler. Sınıflandırıcı olarak *Maksimum Entropi* modeli kullandılar. En iyi 6 öznitelik ile bulunan sonucun doğruluğu, tüm veri seti ile bulunan sonuçla karşılaştırıldı (doğruluk değerindeki en büyük kaybın sadece% 0,04 olduğu gözlemlendi). Azaltılmış özniteliklerin sınıflandırma test sürelerini %47 'ye kadar azalttığını tespit ettiler.

Fatemeh Amiri ve ark. (2011) *doğrusal korelasyon katsayısı* ve *doğrusal olmayan karşılıklı bilgi* olmak üzere iki ÖS algoritması önerdiler. Sınıflandırıcı olarak *En Küçük Kareler Destek Vektör Makinesi* kullanarak bir STS sundular. KDD Cup 99 veri seti üzerinde yapılan deneylerde, önerilen yöntemlerden karşılıklı bilgi tabanlı özellik seçim yönteminin, özellikle R2L ve U2R saldırıları için izinsiz girişleri daha yüksek hassasiyetle bulduğunu tespit ettiler.

Bu çalışmada, sınıflandırma işlemi için sırasıyla izlenen yol aşağıda maddeler halinde sıralanmış ve Şekil 1 de akış şeması görülmektedir.

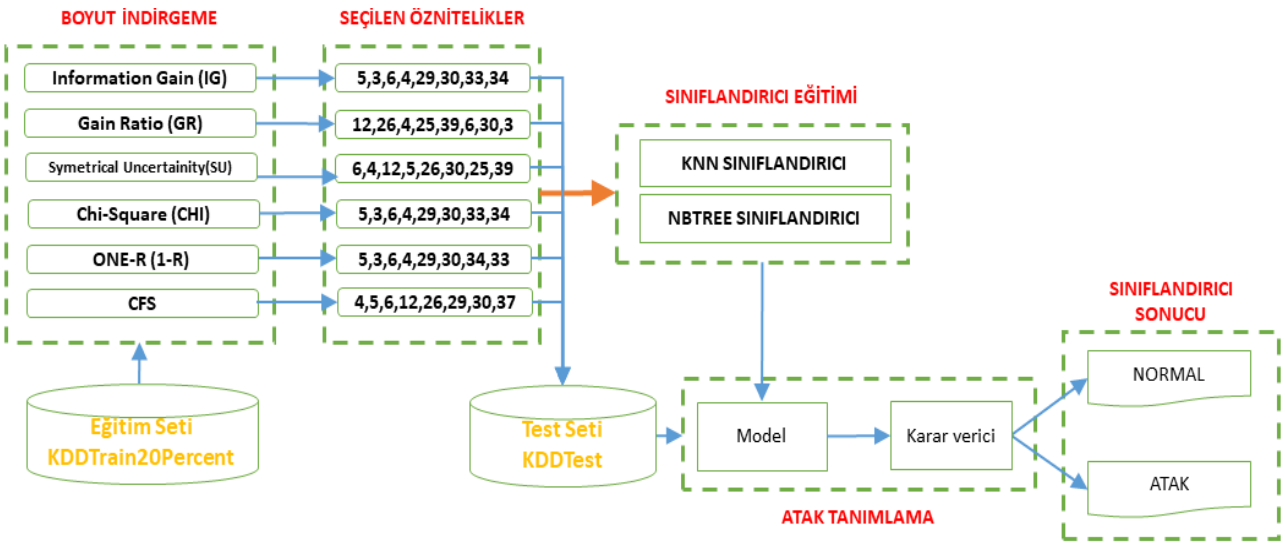
1) Boyut indirgemek için Eğitim seti Öznitelik Seçiciler aracılığıyla işleme alınır.
2) Her bir öznitelik seçiciden sıralama ölçütüne göre 8 adet öznitelik seçilir.
3) Seçilen öznitelikler sınıflandırıcıların eğitimi için kullanılır, aynı zamanda test veri setinden bu 8 öznitelik seçilir.
4) Test seti için seçilen öznitelikler oluşturulan modele sürülür.
5) Model sonucuna göre Karar verici örneğin atak veya normal kayıt olduğunu belirler.

Materyal ve Yöntem

Veri Seti

Bu çalışmada NSLKDD isimli veri kümesi kullanılmıştır. NSLKDD veri seti KDD cup 99 isimli veri setinin yinelenen kayıtlarının silinerek ve yeterli sayıda kayıt alınarak indirgenmiş şeklidir ve birçok çalışmada kullanılmıştır. Veri seti eğitim için KDDTrain ve KDDTrain20Percent isimli dosyalar ve test için KDDTest ve KDDTest21 isimli dosyalar olmak üzere 4 farklı dosya şeklinde indirilebilmektedir. Her bir dosya 41 adet öznitelik içermektedir. Veri setindeki 42. sütunda atak tipleri bulunmaktadır. DOS, Probe, U2R ve R2L olmak üzere 4 sınıf atak mevcuttur.

1.DOS (Denial of Service): mağdurun kaynaklarını tüketen ve böylece meşru talepleri yerine getiremeyen bir saldırı kategorisidir.
2.Probe: saldırılarının amacı, uzaktaki mağdur hakkında bilgi edinmektir.
3.U2R (User to Remote): Kullanıcı ayrıcalıklarına yetkisiz erişim, saldırganın kurban sistemine giriş yapmak için normal bir hesap kullandığı ve kurbanda bir güvenlik açığından yararlanarak yönetici ayrıcalıkları kazanmaya çalıştığı bir saldırı türüdür.
4.R2L (Remote to Local): uzaktaki bir makineden yetkisiz erişim, saldırgan uzaktaki bir makineye girer ve kurban makinesine yerel olarak erişir.
(L.Dhanabal, Dr. S.P. Shantharajah, 2015)



Şekil 1. *Önerdiğimiz Yöntemin Akış Diyagramı*

Bu çalışmada KDDTrain20Percent veri seti eğitim için KDDTest veri seti test için kullanılmıştır. Tablo 1' de kayıt sayıları gösterilmektedir.

Tablo 1. *Çalışmada kullanılan veri dosyalarına ilişkin Anomali ve Normal Kayıt Sayıları*

Trafik Tipi		KDDTrain20P	KDDTest
Normal		13449	9711
Anomali	DOS	9233	7458
	U2R	11	67
	R2L	347	2887
	PROBE	2289	2421
TOPLAM		**25329**	**22544**

Tablo 2' de atak tipleri sınıflara göre listelenmiştir. Eğitim setinde bulunan bazı atak tiplerinin test setinde bulunmaması, çalışmanın anomali tespitinde sıfırıncı gün saldırılarının tespit edilmesine karşı hassasiyetini göstermektedir.

Tablo 2. *Çalışmada kullanılan veri dosyalarına ilişkin Atak Sınıfları ve Tipleri*

Atak Sınıfı	KDDTrain20Percent Atak Tipleri	KDDTest Atak Tipleri
DoS	Back, Land, Neptune, Pod, Smurf,Teardrop (6)	Back, Land, Neptune, Pod,Smurf,Teardrop,**Apache2, Udpstorm, Processtable, Worm** (10)
Probe	Ipsweep, Nmap, Portsweep, Satan (4)	Satan, Ipsweep, Nmap, Portsweep, **Mscan, Saint** (6)
R2L	Guess_Password, Ftp_write, Imap, Phf, Multihop, Warezmaster, Warezclient, Spy, (8)	Guess_Password, Ftp_write, Imap, Phf, Multihop, Warezmaster, Warezclient, Spy, **Xlock, Xsnoop, Snmpguess, Snmpgetattack, Httptunnel, Sendmail, Named** (16)
U2R	Buffer_overflow, Loadmodule, Rootkit, Perl, (4)	Buffer_overflow, Loadmodule, Rootkit, Perl,**Sqlattack, Xterm, Ps** (7)

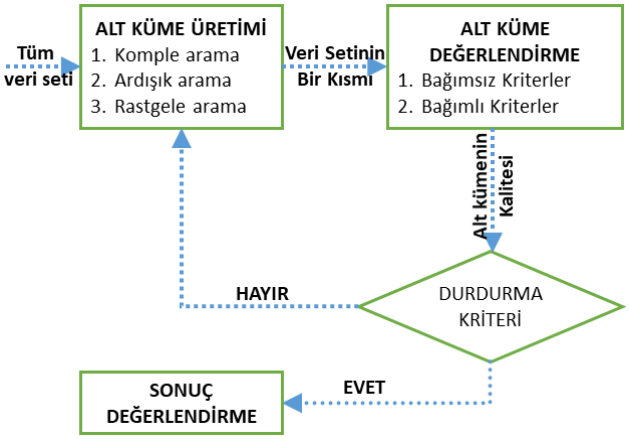
Tablo 3 'te NSLKDD veri setindeki tüm öznitelikler sunulmuştur.

Tablo 3. *NSLKDD veri seti öznitelikleri*

Öznitelik No	Öznitelik Adı
1	Duration
2	Protocol-type
3	Service
4	Flag
5	Src-bytes
6	Dst-bytes
7	Land
8	Wrong-fragment
9	Urgent
10	Hot
11	Num-failed-logins
12	Logged-in
13	Num-compromised
14	Root-shell
15	Su-attempted
16	Num-root
17	Num-file-creations
18	Num-shells
19	Num-access-files
20	Num-outbound-cmds
21	Is-host-login
22	Is-guest-login
23	Count
24	Srv-count
25	Serror-rate
26	Srv-serror-rate
27	Rerror-rate
28	Srv-rerror-rate
29	Same-srv-rate
30	Diff-srv-rate
31	Srv-diff-host-rate
32	Dst-host-count
33	Dst-host-srv-count
34	Dst-host-same-srv-rate
35	Dst-host-diff-srv-rate
36	Dst-host-same-src-portrate
37	Dst-host-srv-diff-hostrate
38	Dst-host-serror-rate
39	Dst-host-srv-serror-rate
40	Dst-host-rerror-rate
41	Dst-host-srv-rerror-rate

Filtre Tabanlı Öznitelik Seçme Yöntemleri

Öznitelik seçimi, en basit tanımıyla seçim yapılacak veri setini temsil edebilecek en iyi özniteliklerin belirlenmesidir. ÖS aynı zamanda bir veri indirgeme yöntemidir. Ağ akış verilerinde anomali tespiti için veri boyutunun azaltılması sistemin işlem yükünün azaltılması, ilgisiz verilerin elenmesi ve model başarısının arttırılması için kritik öneme sahiptir. ÖS 4 temel adımdan oluşmaktadır.



Şekil 2. *Öznitelik Seçimi Genel Akışı*

Alt Küme Üretimi - Arama uzayındaki her durumun değerlendirme aşaması için bir aday alt kümeyi belirlediği temel bir sezgisel arama sürecidir. D adet özniteliğe sahip bir veri seti için 2^D adet aday alt küme söz konusudur. D' nin artmasıyla arama işlemi zorlaşmaktadır. Bu durumun önüne geçmek için komple arama, ardışık arama ve rastgele arama gibi farklı yöntemler kullanılmaktadır.

Alt Küme Değerlendirme - Birinci adımda oluşturulan tüm altkümeler bağımlı ve bağımsız ölçütlere göre değerlendirilerek en iyi alt küme seçilir. Filtreleme tabanlı yöntemlerde genellikle bağımsız ölçütler kullanılır.

Durdurma Ölçütü - Arama işleminin bitmesi, minimum öznitelik veya maximum iterasyon sayısına ulaşılması, yeterince iyi bir alt kümenin elde edilmesi gibi kullanıcı tarafından belirlenen ölçütler aracılığıyla ÖS sürecini durduran adımdır.

Sonuç Değerlendirme - Veriler hakkında önsel bilgileri kullanarak çıktıyı tahmin etme adımıdır (Nour M., Jiankun H., Jill S., 2019).

Öznitelik seçimi; filtreleme tabanlı yöntemler, sarmal yöntemler ve gömülü yöntemler olmak üzere 3 başlıkta incelenir.

Bu çalışmada özntelik seçimi yöntemlerinden filtreleme tabanlı olan *Bilgi Kazancı, Kazanç oranı, Simetrik Belirsizlik Katsayısı, Ki-Kare, One-R, Korelasyon Tabanlı* ÖS yöntemlerinin STS 'lerin başarımına etkisi araştırılmıştır.
Çalışmada kullandığımız ilk 3 yöntem Entropi tabanlı yöntemlerdir. Entropi, bir sistemin belirsizliğinin bir ölçüsüdür. p(y), veri kümesindeki y. veri sınıfının tüm sınıf içerisindeki bulunma olasılığını ifade etmek üzere, bir Y öznitelik vektörünün entropisi formül 1 'deki sekilde hesaplanır.

$$H(Y) = -\sum_{y \epsilon Y} p(y)\, log_2(p(y)) \qquad (1)$$

Bir Y özniteliğini tanımlarken bir X özniteliği de kullanılıyorsa Y ile X arasında formül 2 'deki gibi bir ilişki söz konusu olacaktır.

$$H(Y|X) = -\sum_{x \epsilon X} p(x) \sum_{y \epsilon Y} p(y|x)\, log_2(p(y|x)) \qquad (2)$$

a) Bilgi Kazancı (BK)

Entropi teorisine dayanan bir yöntemdir. X özelliğine bağlı olarak Y özelliğinin entropi değerindeki azalmayı gösterir. BK formül 4 'te gösterildiği şekilde hesaplanır.

$$Bilgi\ Kazancı = H(Y) - H(Y|X) \qquad (3)$$

Yöntemin zayıf yanı, daha fazla bilgiye sahip olmasa bile çok çeşitli değerlere sahip özellikler lehine önyargılı şekilde sonuç vermesidir. [(Budak H., 2018), (Jasmina N., 2016)]

b) Kazanç Oranı (KO)

Kazanç oranı; Bilgi Kazancı yönteminin açığı olan çeşitliliğe karşı X özniteliğinin entropisi vasıtasıyla normalize edilmesiyle elde edilir [(Budak H. , 2018), (Jasmina N. , 2016)]. KO formül 4 'te gösterildiği şekilde hesaplanır.

$$Kazanç\ Oranı = \frac{Bilgi\ Kazancı}{H(X)} \qquad (4)$$

c) Simetrik Belirsizlik Katsayısı (SBK)

Kazanç oranındaki gibi Bilgi Kazancı yönteminin zayıf yanını X ve Y özniteliklerinin entropilerinin toplamı vasıtasıyla normalize edilmesi sonucu elde edilir [(Budak H., 2018), (Jasmina N., 2016)]. SBK formül 5 'te gösterildiği şekilde hesaplanır.

$$SBK = 2 * \frac{Bilgi\ Kazancı}{H(Y) + H(X)} \quad (5)$$

d) Ki-Kare (Ki)

Ki-Kare testi gözlenen ve beklenen frekanslar arasındaki ilişkiye dayanan 2 aşamalı bir istatistiksel yöntemdir. İlk aşamada gözlenen değerlerin gerçek sınıflara göre ki-kare X^2 istatistiği hesaplanır. İkinci aşamada testi yapan tarafından belirlenen önemlilik seviyesi yüzdesi ve veri setindeki öznitelik sayısının 1 eksiği olan serbestlik derecesi referans alınarak bir seçim yapılır. X^2 değerin sıfıra yaklaşması gözlenen ve beklenen frekans değerlerinin uyumluluğu, sıfırdan çok büyük olması uyumsuzluğu işaret etmektedir [(Budak H., 2018), (Kaynar O. Ve ark ,2018)]. Ki formül 6 'da gösterildiği şekilde hesaplanır.

$$X^2 = \sum_{i=1}^{n} \frac{(o_i - e_i)^2}{e_i} \quad (6)$$

n ; veri setindeki öznitelik sayısını,
o_i; i'inci öznitelik için gözlenen frekans değeri
e_i; i'inci öznitelik için beklenen frekans değeri

e) One-R (1-R)

One-R yöntemi, eğitim setindeki her bir özniteliğin algoritma tarafından oluşturulan kurala göre sınıflandırılıp sınıflandırma hata oranına göre sıralama yapma esasına dayanır. (Morariu, D. ve ark.)

One-R algoritma adımları kısaca sözel olarak aşağıdaki gibi ifade edilebilir.

Her bir özellik f için,
f nin etki alanındaki her v değeri için,
v değerine sahip f özellik örnek setini seç,
c = seçilen sette en sık rastlanan sınıf değeri,
her bir f özelliği için "f özelliği v değerini alıyorsa sınıfı c" kuralını ekle,

En yüksek sınıflandırma oranına sahip kuralı çıktı olarak üret.

f) Korelasyon Tabanlı ÖS (KTÖS)

Korelasyon temelli bir değerlendirme işlevine göre öznitelik altkümelerini sıralayan basit bir filtre algoritmasıdır. Yöntem, sınıf etiketiyle yüksek korelasyon gösteren ve birbirleriyle ilişkisiz öznitelikler içeren alt kümeleri bulma esasına dayanır. İlgisiz öznitelikler düşük, birbirinin aynı veya dengi öznitelikler ise yüksek korelasyon göstereceklerinden dolayı elenmelidir (Hall, M. A., 1999). KTÖS formül 7 'de gösterildiği şekilde hesaplanır.

$$M_S = \frac{kr_{cf}}{\sqrt{k + k(k-1)r_{ff}}} \quad (7)$$

M_S= k adet öznitelik içeren S altkümesinin fayda değeri

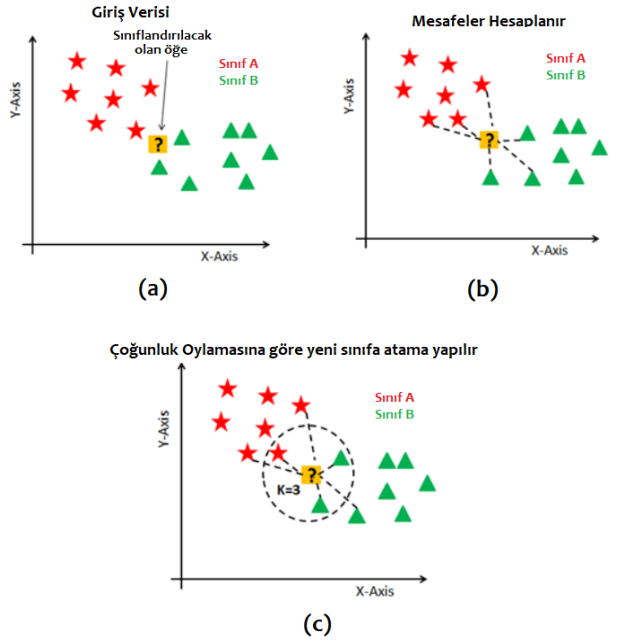
r_{cf}= Sınıf etiketi ile ilgili öznitelik arasındaki korelasyon

r_{ff}= Özniteliklerin birbirleri arasındaki korelasyon

Sınıflandırma ve Başarı Ölçütü

Bu çalışmada NSLKDD veri setinin filtreleme tabanlı 6 farklı ÖS yöntemiyle boyutu indirgenmiştir. Her yöntemden sıralama usulüne göre en başarılı 8 öznitelik seçilmiştir. Elde edilen son öznitelik vektörlerinin sistemin başarımına etkisini incelemek için k En Yakın Komşu ve Rastgele Orman olmak üzere 2 farklı sınıflandırıcı kullanılmıştır.

a) k-En Yakın Komşu algoritması bilinmeyen bir nesnenin (Şekil. 3-a) mesafe ölçüm değerine göre (Şekil. 3-b) hangi sınıfa ait olduğuna karar veren basit bir öğrenme algoritmasıdır. En bilinen mesafe ölçüm yöntemleri Öklid, Mahalanobis, Minkowski, Manhattan' dır. KNN algoritmasında k komşuluk değeri seçilir ve sonra bilinmeyen nesne çoğunluk kuralına göre ilgili sınıfa atanır (Şekil. 3-c), (Luis A. Berrueta ve ark., 2007).



Şekil 3. *KNN algoritmasının X-Y ekseninde gösterimi*

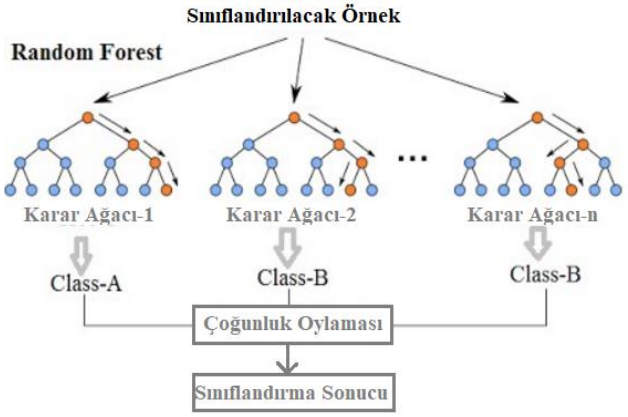
b) Rastgele Orman algoritması, bir karar ağacı sınıflandırma yöntemidir. RO, her karar ağacının sınıflandırıcı modeline tek bir oyla katkıda bulunduğu bir sınıflandırma ağaçları topluluğu olarak tanımlanabilir. Bu ağacın her bir ara düğümü ile öznitelikler sınanmakta ve sınama sonucu dallarla ifade edilmektedir. Ağacın yaprakları ise sınıfları temsil etmektedir. Diğer makine öğrenme metotlarına kıyasla özelleştirilmesi gereken parametre sayısı daha azdır [(Zhou, Y ve ark.,2019), (Aydın, A. ve ark., 2018)]

RF' de, bireysel ağaç yapılı sınıflandırıcı topluluğu 8 'deki gibi ifade edilir.

$$\{h(x, \Theta_k), k = 1,2, \dots i \dots\} \quad (8)$$

h, Rastgele orman sınıflandırıcı
Θ_k, Bağımsız olarak aynı şekilde dağıtılan rastgele vektörleri ifade eder.
x, her ağacın sınıf etiketini temsil eder.

Rastgele Orman algoritması düşük hesaplama yüküne sahiptir ve aykırı parametrelere duyarsızdır. Ayrıca, aşırı öğrenme bireysel karar ağacına kıyasla daha az sorun teşkil eder ve iş yükünü arttıran bir işlem olan ağaçları budamaya gerek yoktur.



Şekil 4. *RF algoritmasın genel akış şeması*

Değerlendirme Ölçütleri

STS 'lerin değerlendirme ölçütleri için bugüne kadar maalesef tam olarak bir referans ölçü belirlenememiştir. Literatürde 2000-2008 yılları arasında yapılan çalışmaların %42 'sinde Pozitif Doğru Oranı-Algılama Oranı (True Positive Rate-TPR, Detection Rate-**DR**), Pozitif Yanlış Oranı-Yanlış Alarm Oranı (False Positive Rate-FPR, False Alarm Rate-**FAR**) ve Eğri Altındaki Alan (Area Under **R**eceiver **O**perator **C**haracteristic Curve-**AUC**) değerleri kullanılmıştır. Ek olarak Doğruluk (Accuracy) değeri de bu çalışma kapsamında kullanılmıştır (Kumar, G., 2014). Bu çalışmada ***DR***, ***FAR***, ***ACC*** ve ***AUC*** kısaltmaları kullanılacaktır.

Tablo 4. *Konfüzyon Matrisi*

		Tahmin Edilen Sınıf	
		Normal	**Atak**
Asıl Sınıf	**Normal**	TN	FP
	Atak	FN	TP

TP-Atak olarak tahmin edilen atak örneği
TN-Normal olarak tahmin edilen Normal örnek
FP-Atak olarak tahmin edilen Normal örnek
FN-Normal olarak tespit edilen Atak örneği adetlerini ifade etmek üzere; (Milan, 2018)

$$DR = TPR = \frac{TP}{TP + FN} \quad (9)$$

$$FAR = FPR = \frac{TP}{TP + FN} \quad (10)$$

$$ACC = \frac{TP + TN}{TP + TN + FP + FN} \quad (11)$$

Uygulama

Bu çalışmada NSLKDD veri setinin filtreleme tabanlı 6 farklı ÖS yöntemiyle boyutu indirgenmiştir. KDDTrain20Percent isimli veriler eğitim amaçlı kullanılarak sınıflandırıcı modeli oluşturulmuştur. Her yöntem için 8 adet öznitelik seçilmiştir. Öte yandan her bir ÖS yöntemi ile sıralama değerlerine göre elde edilen en iyi 8 öznitelik KDDTest verilerinden seçilerek bu öznitelikler sınıflandırıcıya sürülmüştür. Öznitelik seçimi yapılmadan tüm öznitelikler de ayrıca sınıflandırma işletmine tabi tutulmuştur.

Elde edilen öznitelik vektörlerinin sistemin başarımına etkisini incelemek için KNN ve Random Forest olmak üzere 2 farklı sınıflandırıcı kullanılmıştır. Sınıflandırıcı çıkışında girişe verilen örnekler ***Normal*** veya ***Atak*** olarak etiketlenmiştir.

Her bir ÖS yöntemi ile seçilen öznitelikler ve sıralamadaki değerleri Tablo 5 'te sunulmuştur. Tablo 5 'ten görüleceği üzere 1R, IG ve CHI yöntemleri ile seçilen özniteliklerin sıralamadaki yerleri farklı olsa da aynı özniteliklerdir. Dolayısıyla sınıflandırma sonucunda elde edilecek parametreler aynı olacaktır.

Tablo 5. *ÖS yöntemleri ile elde edilen sonuçlar ve sıralanması*

1-R	**KO**
Sıralanan Öznitelikler:	Sıralanan Öznitelikler:
96,28453 5 src_bytes	0,415094 12 logged_in
91,4457 3 service	0,371408 26 srv_serror_rate
91,05272 6 dst_bytes	0,340202 4 flag
88,15497 4 flag	0,336928 25 serror_rate
87,28168 29 same_srv_rate	0,331043 39 dst_host_srv_serror_rate
87,14274 30 diff_srv_rate	0,32372 6 dst_bytes
85,28898 34 dst_host_same_srv_rate	0,279661 30 diff_srv_rate
84,72531 33 dst_host_srv_count	0,27736 38 dst_host_serror_rate
BK	**SBK**
Sıralanan Öznitelikler:	Sıralanan Öznitelikler:
0,806777083 5 src_bytes	0,428608284 6 dst_bytes
0,672035304 3 service	0,411671627 4 flag
0,631947382 6 dst_bytes	0,408991802 12 logged_in
0,519431475 4 flag	0,394991205 5 src_bytes
0,515902949 30 diff_srv_rate	0,374936398 26 srv_serror_rate
0,507754237 29 same_srv_rate	0,363128634 30 diff_srv_rate
0,47284563 33 dst_host_srv_count	0,362298577 25 serror_rate
0,43902981 34 dst_host_same_srv_rate	0,361221335 39 dst_host_srv_serror_rate
Ki	**KTÖS**
Sıralanan Öznitelikler:	Sıralanan Öznitelikler: 4,5,6,12,26,29,30,37 : 8
21786,70275 5 src_bytes	flag
18639,26163 3 service	src_bytes
17581,01415 6 dst_bytes	dst_bytes
15153,70136 4 flag	logged_in
14723,01823 29 same_srv_rate	srv_serror_rate
14715,62593 30 diff_srv_rate	same_srv_rate
13897,27784 33 dst_host_srv_count	diff_srv_rate
13402,85782 34 dst_host_same_srv_rate	dst_host_srv_diff_host_rate

1-R ve Ki yöntemleri ile yapılan seçimde tüm sıralama aynı olup sadece 7 ve 8nci sıradaki *dst_host_srv_count* ve *dst_host_same_srv_rate* özniteliklerinin yerleri farklıdır. BK ve Ki yöntemleri ile yapılan seçimde ise tüm sıralama aynı olup sadece 5 ve 6ncı sıradaki *diff_srv_rate* ve *same_srv_rate* özniteliklerinin yerleri farklıdır. *Flag, src_bytes, dst_bytes* ve *diff_srv_rate* öznitelikleri tüm yöntemlerde en iyi 8 öznitelik arasında bulunmuştur.

Deneyler WEKA 3.8.3 versiyonu ile 2.6 GHz Intel Core i7-4510U işlemci, 8 GB RAM özelliklerinde diz üstü bilgisayar ile gerçekleştirilmiştir.

Sonuçlar ve Tartışma

Bu çalışmada filtreleme tabanlı öznitelik seçme yöntemlerinin STS 'lere etkisi araştırılmıştır. Literatürde çoğunlukla aynı veri seti ile yapılan birçok çalışma mevcuttur. Bu çalışmada eğitim ve test için farklı veri setleri kullanıldığından ötürü farklılık arz etmektedir. Çalışmada önce ham veri, ardından ÖS yöntemleri kullanılarak elde edilen öznitelikler KNN ve RO algoritmalarıyla sınıflandırılmış ve sonuçlar Tablo 6'da sunulmuştur.

STS 'lerin değerlendirme ölçütleri için bugüne kadar tam bir referans ölçü belirlenmemiştir. Literatürde çoğunlukla kullanılan ***DR***, ***FAR***, ***AUC*** ve ***ACC*** parametreleri değerlendirme ölçütleri olarak kullanılmıştır. Değerlendirme yapılırken BK/Ki/1-R ÖS yöntemleri aynı öznitelikleri barındırdığından bu 3 yöntem bir arada anılacaktır.

Sonuçlar sınıflandırma doğruluğu bakımından değerlendirilince RO 'nun KNN 'ye göre üstünlüğü göze çarpmaktadır. En yüksek ACC değeri BK/Ki/1-R yöntemleri sonucu elde edilen öznitelikler kullanılarak RO algoritması sınıflandırması ile %83,31 olarak elde edilmiştir. Ayrıca aynı yöntemle elde edilen DR değeri %74,05, FAR değeri %4,46 ile tüm değerler arasında kabul edilebilir düzeyde olup en önemli ölçüt olan AUC değeri %93,40 ile oldukça başarılı bir seviyededir.

RO ile elde edilen AUC değerleri KNN ile elde edilen AUC değerlerine göre bariz oranda üstünlüğü göze çarpmaktadır.

ÖS yöntemleri bakımından BK/Ki/1-R yöntemleri AUC ve FAR bakımından ham veri sonuçlarına göre az miktarda olumsuz yönde farklılık göstermiş olmakla birlikte ACC ve DR değerleri bakımından daha başarılıdır.

İşlem süreleri bakımından incelendiğinde RO algoritmasının KNN algoritmasına göre üstünlüğü açıkça görülmektedir. RO ile yapılan sınıflandırma süreleri KNN ile yapılan sınıflandırma sürelerinde göre 6 – 8 kat daha düşüktür. Yine işlem süreleri ham veri setine karşılık ÖS sonucu elde edilen öznitelikler ile karşılaştırınca ÖS ile veri boyutunun düşmesinden ötürü işlemler beklendiği şekilde daha düşük sürelerde gerçekleşmiştir. BK/Ki/1-R yöntemleriyle 3,09 sn. sürede elde edilen %83,31 ACC değeri tüm yöntemler arasında en yüksek değer olup %74,05 DR değeri RO algoritmasındaki en yüksek değeri vermiştir. Ayrıca aynı yöntemle elde edilen %4,46 FAR değeri ile %93,40 AUC değerleri de kabul edilebilir düzeydedir.

Tüm sonuçlar değerlendirilince BK/Ki/1-R özniteliklerinin RO ile sınıflandırılması en optimum yöntem olduğu rahatlıkla ifade edilebilir. Bu sonuçlara göre ÖS yöntemlerinin STS sistemlerine olumlu yönde katkı sağlandığı sonucuna varılmaktadır.

Tablo 6. *ÖS yöntemleri sonucu elde edilen özniteliklerin KNN ve RF ile sınıflandırma sonuçları*

		KNN					RANDOM FOREST				
Ö.S. Metodu	**Seçilen Öznitelikler**	**İşlem süresi (sn)**	**ACC %**	**DR %**	**FAR %**	**AUC %**	**İşlem süresi (sn)**	**ACC %**	**DR %**	**FAR %**	**AUC %**
Ham	Tüm Öznitelikler	58,92	80,36	68,39	3,80	82,30	7,57	80,54	67,92	**2,70**	***95,60***
IG	5,3,6,4,30,29,33,34	20,93	79,64	67,47	4,27	82,00	3,09	***83,31***	**74,05**	4,46	93,40
GR	12,26,4,25,39,6,30,38	32,25	**82,81**	***75,42***	7,42	**89,60**	4,35	81,42	72,84	7,23	91,00
SU	6,4,12,5,26,30,25,39	25,50	81,14	69,38	3,31	82,80	4,37	77,59	63,16	3,33	90,30
CHI	5,3,6,4,29,30,33,34	20,93	79,64	67,47	4,27	82,00	3,09	83,31	74,05	4,46	93,40
ONE-R	5,3,6,4,29,30,34,33	20,93	79,64	67,47	4,27	82,00	3,09	83,31	74,05	4,46	93,40
CFS	4,5,6,12,26,29,30,37	43,15	77,18	66,41	***2,54***	78,40	4,85	76,62	61,43	3,28	92,20

Kaynaklar

Alazab, A., Hobbs, M., Abawajy, J., & Alazab, M. (2012) "Using feature selection for intrusion detection system." In Communications and Information Technologies (ISCIT), 2012 International Symposium on (pp. 296-301). IEEE.

Aydın, A., Doğru, İ. A., & Dörterler, M. (2018). Makine Öğrenmesi Algoritmalarıyla Android Kötücül Yazılım Uygulamalarının Tespiti. Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 22(2), 1087-1094.

Budak H., (2018), "Özellik Seçim Yöntemleri ve Yeni Bir Yaklaşım", Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi Cilt 22, Özel Sayı, 21-31

F. Amiri, M.R. Yousefi, C. Lucas, A. Shakery, N. Yazdani, (2011) "Mutual information-based feature selection for intrusion detection systems," Journal of Network and Computer Applications, 34, pp.1184–1199.

Hall, M. A. (1999), "Correlation-based feature selection for machine learning."

Kaynar O., Arslan H., Görmez Y., Işık Y.E., (2018), "Makine Öğrenmesi ve Öznitelik Seçim Yöntemleriyle Saldırı Tespiti", Bilişim Teknolojileri Dergisi, Cilt: 11, Sayı: 2

Kumar, G. (2014). Evaluation metrics for intrusion detection systems-a study. Evaluation, 2(11).

L. Dhanabal, Dr. S.P. Shantharajah, (2015) "A Study on NSL-KDD Dataset for Intrusion Detection System Based on Classification Algorithms" International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 6, June 2015.

Lee, S.M., Kim, D.S. and Park, J.S. (2012) "A survey and taxonomy of lightweight intrusion detection systems", Journal of Internet Services and Information Security, Vol. 2, No. 1/2, pp.119–131.

Li, Y., Fang, B. X., Chen, Y., & Guo, L. (2006) "A lightweight intrusion detection model based on feature selection and maximum entropy model." In Communication Technology. ICCT'06. International Conference on (pp. 1-4). IEEE.

Luis A. Berrueta, Rosa M. Alonso-Salces, K´aroly H´eberger (2007), "Supervised pattern recognition in food analysis." Journal of Chromatography A, 1158 (2007) 196–214.

Milan, H. Sardana, K. Singh (2018), Reducing False Alarms in Intrusion Detection Systems – A Survey, International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056

Morariu, D., R. Cretulescu, Macarie Breazu. (2013) "Feature Selection in Document Classification." The fourth International Conference in Romania of Information Science and Information Literacy.

Nour M., Jiankun H., Jill S., (2019) "A holistic review of Network Anomaly Detection Systems: A comprehensive survey", Journal of Network and Computer Applications 128 (2019) 33–55

Novaković, Jasmina. (2016) "Toward optimal feature selection using ranking methods and classification algorithms." Yugoslav Journal of Operations Research 21.1

Zhou, Y. Y., & Cheng, G. (2019). An Efficient Network Intrusion Detection System Based on Feature Selection and Ensemble Classifier. arXiv preprint arXiv:1904.01352.

(https://www.unb.ca/cic/datasets/nsl.html)

Effect of Filter Based Feature Selection Methods to Network Anomaly Detection Systems

Extended abstract

Information security of systems is provided via the use of authentication, antivirus programs, firewalls, intrusion prevention systems as alone or in combination. The protection capability of such security systems depends on which the databases are updated. Preventing attacks called zero-day attacks, which the databases have never seen before, is possible by the continuous monitoring of the movements of the system and the detection of abnormal conditions rather than by rule-based systems. This turns the anomaly-based network security into a classification problem.

In this study, it is aimed to research the effect of filter based Feature Selection (FS) Methods to Network Anomaly Detection Systems (NADS). The NSLKDD data set was used in this paper. There are 41 features in NSLKDD dataset. NSLKDD data set contains 4 data folder named KDDTrain, KDDTrain20Percent, KDDTest, KDDTest21. In this paper KDDTrain20Percent folder is used for training while KDDTest folder is used for testing. Thus, the robustness of the system has been proven by testing with a data set and testing with another data set.

In this study, firstly dimensionality is reduced by using filter-based feature selection methods [Information Gain (IG), Gain Ratio (GR), Symmetrical Uncertainty (SU), Chi-Square (CHI), One-R (1-R) and Correlation Based Feature Selection (CFS)]. On each FS method, according to ranking rule the most effective 8 features were selected from the training set. Then these selected 8 features also selected on the test set for driving to the classifiers as the final data set. Even though the same 8 features selected with IG, CHI and 1-R methods, the ranking of features were different. 4 common feature was selected for all methods named flag, src_bytes, dst_bytes and diff_srv_rate.

Final feature vectors are classified by using k-Nearest Neighbor (KNN) and Random Forest (RF) classifiers.

k-Nearest Neighborhood (KNN) is a non-parametric learning algorithm based on the principle of determining which class an unknown object belongs according to distance measurement. The most common distance measurement methods are Euclidean, Mahalanobis, Minkowski, Manhattan etc. In the KNN algorithm k neighborhood value is chosen and then the unknown object is assigned based on majority rule to the lowest distance class.

Random Forest(RF) is a decision tree technique that operates by constructing multiple decision trees. RF can be described as an ensemble of classification trees where every tree contributes with a single vote for the task of the most frequent class to the input data. Compared to other machine learning methods there are fewer parameters to be specified when running RF.

*Although no benchmark metric exists till date for intrusion detection, as per statistics of a survey of 276 papers published between 2000-2008, 42% of the papers accessed performance of the systems by using **DR**, **FPR** and area under the ROC (**AUC**). Additionally **process time** and accuracy **ACC** values were used for evaluating the performance of the methods.*

By means of classifier RF is more superior than KNN. Especially on AUC value, this difference clearly can be seen. The mean AUC of all methods is %82,73 for KNN, while it is %92,76 for RF. Mean values of other evaluation metrics are listed below.

	KNN	*RF*
ACC	*%80,06*	*%80,87*
DR	*%68,86*	*%69,64*
FAR	*%4,27*	*%4,27*
Process Time	*31,80 sec*	*4,34 sec*

By means of FS method, the features selected with IG/CHI/1-R are better than other methods. The best ACC is achieved %83,31 on RF classifier and the best AUC is achieved %93,40 among FS methods. DR and FAR values are also reasonable.

By means of processing time, RF is clearly better than KNN for all methods. When compared to the raw features and reduced features with FS methods the processing time is decreased both KNN and RF as expected.

The results showed that FS methods have positive effect to NADSs.

Keywords: *Filter based fetaure selection, Network anomaly detection system*