ISSN: 2146-8168 Sayı: **11**, Yıl: **2015**, Sayfa: **21-40** **http://bilader.gop.edu.tr**

Gaziosmanpaşa Üniversitesi
Fen Bilimleri Enstitüsü
Gaziosmanpaşa Bilimsel Araştırma Dergisi

Dergiye Geliş Tarihi: 22.06.2015 *Baş Editör*: Bilge Hilal ÇADIRCI
Yayına Kabul Tarihi: 18.08.2015 *Alan Editörü*: Levent GÖKREM

Yapay Sinir Ağları Kullanarak, Bilgisayar Ağlarında Saldırı Tespit Sistemi ve Başarımlarının İncelenmesi

Vedat MARTTİN[a,1] (vedatmarttin@gmail.com)
Nazım İMAL[b] (nazim.imal@bilecik.edu.tr)

[a] *Bilecik Şeyh Edebali Üniversitesi, Fen Bilimleri Enstitüsü-Bilgisayar Müh.ABD , 11210 Bilecik*
[b] *Bilecik Şeyh Edebali Üniversitesi, Elektrik-Elektronik Müh.Bölümü, 11210 Bilecik*

Özet – Her geçen gün önemi artan bilgi ve ağ üzerindeki bilgi sistemlerine yapılan saldırıların tespit edilmesinde kullanılan saldırı tespit sistemleri (STS) Yapay Sinir Ağları (YSA) kullanılarak ele alınmıştır. STS'lerin oluşturulmasında KDD'99 (Knowledge Discovery and Data Mining Tools Competition) veri kümesi kullanılmıştır. Geliştirilen modelin elde edilen başarım sonuçları ile benzer konuda çalışacak araştırmacılara önerilerde bulunulmuştur. Eğitilen YSA ile KDD'99 tarafından oluşturulan örnek veri kümeleri test edilmiş ve bir sınıflandırma algoritması olan YSA'nın, bilinmeyen saldırıları başarılı bir şekilde tespit ettiği gözlenmiştir.

Anahtar Kelimeler – *Yapay sinir ağları (YSA), Çok katmanlı algılayıcı, (ÇKA) saldırı tespit sistemleri (STS), DoS saldırıları, KDD'99.*

Gaziosmanpaşa Journal of Scientific Research 11 (2015) 21-40

Using Neural Network, In Computer Networks Intrusion Detection System And Study Of Achievements

Abstract – Increasingly important with each passing day, in detecting the attack to knowledge and information systems on the network, intrusion detection systems (STS) used, with Artificial Neural Networks (ANN) are have dealt. In forming IDS, the data set of KDD'99 (Discoverer of Knowledge and Data Mining Tools Competition) was used. With performance results obtained from the developed model, suggestions are made to the researchers will work similar to it. With trained ANN, data sets of instance by created KDD'99 was tested and ANN that is classification algorithm, was observed successfully for detecting unknown attacks.

Keywords – *Artificial neural networks (ANN), Multi layer perceptron (MLP), Intrusion detection system (IDS), DoS attacks, KDD'99.*

Received: 22.06.2015 *Accepted*: 18.08.2015

[1] **Vedat Marttin-*Bilecik Şeyh Edebali Üniversitesi, Fen Bilimleri Enstitüsü-Bilgisayar Müh. ABD , 11210 Bilecik***

1. Giriş

Günümüz teknoloji dünyasında önemli bir yer tutan bilgi ve bilgisayar sistemleri, internetin de sağladığı küresel ölçüler içerisinde yeni boyutlara ulaşmıştır. İnsanlar işlerini büyük ölçüde kolaylaştıran bilgi teknolojilerinden yararlanırken güvenliği de ihmal edilmemelidir. Günümüzde kullanıcıların sosyal medya hesaplarından tutun da devletlerin sırlarının bile bazı web sayfalarında paylaşıldığı görülebilmektedir. Başka bir açıdan bakıldığında bazı kişiler ki, bunlar çeşitli sebeplerle kurumsal yada özel web sitelerine sistem sorumlusundan habersiz sızma yoluyla (hacking) ya da mevcut sistemin zafiyetlerini araştırarak–denemeler yaparak veya köle bilgisayarlar (zombi) yaptırarak müdahale etmektedir. Saldırının olduğu yerde saldırıya karşı savunma da gerekli olduğu için, meydana getirilen saldırıların boyutlarına göre gerekli önlemleri almak gereklidir. Saldırının türüne göre tespit etme ve önlem almak adına saldırı tespit sistemleri (STS-IDS) ve saldırı önleme sistemleri (SÖS-IPS) geliştirilmiştir.

Literatür çalışması yapıldığında STS ve sınıflandırma kapsamında Moradi ve Zulkernine [3], STS uygulamalarında çevrimdışı ağ kullanarak çok katmanlı ağ (MLP) yapının saldırı sınıflandırmasında YSA ile başarılı sonuçlar alınabileceğini göstermiştir. Güven [4], çalışmasında Erol [5] ile benzer şekilde STS'leri detaylı sınıflandırılması ve KDD'99 veri kümesinin meydana gelmesinde kullanılan yöntemin benzerini kullanmıştır. Cannady [6] ve Ryan [7] kendi veri setlerini ele alarak ÇKA yapısı kullanmış ve elde edilen veri kümesindeki özellik sayısında farklılıkları ele almışlardır. Mukkamala [2] ve Güven[4], KDD'99 veri kümesinin tüm veri değerlerini, farklı ÇKA yapısını ile deneyerek buldukları başarımları ele almışlardır. Güven[4] örnekleme sayısını sabit tutarak, KDD'99 daki farklı saldırıları sınıflandırmaya çalışmıştır. Mukkamala [2], çalışmalarında elde ettiği yüksek başarım oranın bulunmasında, ÇKA / DVM'nin birlikte çalıştırılmasından kaynaklandığı görülmüştür. Sammany[8] DARPA'99 veri kümesinde, ÇKA yapısında farklı katman ve daha az özellik kullanarak başarım gerçekleştirmiştir. Tanrıkulu [8] DARPA'98 veri kümesini kullanarak, internet ortamından elde ettikleri saldırı dosyalarını IP adreslerini 4 ayrı özellik olarak ele alıp, 2 farklı yöntem ve denemelerle başarımlar elde etmiştir. Aşağıda önceden ÇKA ile yapılan benzer çalışmaların özet tablosu verilmektedir.

Tablo 1. Önce Yapılan Benzer Çalışmaların Başarım Oranları

Çalışmayı Yapan	YSA Yapısı	İşlem Eleman Sayısı	Veri Seti	Özellik Sayısı	Başarım Oranları (%)
Cannady (1998)	ÇKA	[9 * * 1]	Cannady'in Oluşturduğu Veri Seti	10	91
Ryan (1998)	ÇKA	[100 30 10]	Kendi veri seti	100	96
Mukkamala (2002)	ÇKA, DVM	[41 40 40 1]	KDD'99	41	99,25
Güven (2007)	ÇKA	[41 6 8 1]	KDD'99	41	92,5
Tanrıkulu (2009)	ÇKA	[12 40 40 1]	DARPA '98	5	99,15

2. Saldırı Türleri

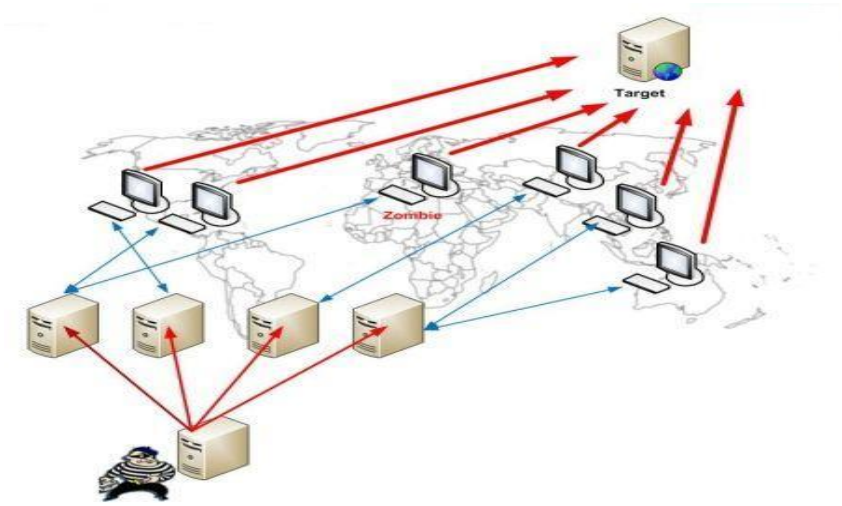
STS'lerin gelişimi sırasında önemli bir yeri olan DARPA veri kümelerinin oluşturulması sırasında belirlenen ve akademik çalışmalarda hala geçerliliğini koruyan saldırı tipleri esas alınmıştır. MIT Lincoln Laboratuarlarında yapılan bu çalışmada, saldırılar bilgisayar sistemine yapılan atak türlerinin kullandıkları yöntemlere göre dört gruba ayrılmış ve DoS (Denial of Service), U2R (User to Root), R2L (Remote to Local) ve Probing olarak adlandırılmıştır [1].

2.1 Hizmet Aksattırma (DoS):

Genellikle hizmetin verilmesi engellenmek istenildiğinde sisteme cevap verebileceğinden çok istek paketleri gönderilmesi ile hedefteki belleği şişirilerek gerçekleştirilen saldırı tipidir. Saldırı ARP tablolarındaki değerleri değiştirmeye yöneliktir.

DARPA veritabanında isimlendirildiği haliyle, en çok bilinen DoS saldırı tipleri, SYN flood, Smurf, UDPstorm, Pingflood, Neptune, Mailbomb gibi saldırılardır [2].

DoS saldırısının dağıtık şekilde pek çok kullanıcı ya da zombi bilgisayarlar tarafında yapılmasıyla DDoS (Distributed Denial Of Service) saldırı tipi gerçekleştirilmektedir.



Şekil 1. Dağıtık Hizmet Aksattırma (DDoS) saldırısı örneği

2.2. Yetki Yükseltme (U2R)

U2R saldırıları, kullanıcıların normal yetkilere sahip olan kendi hesaplarından oturum açtıktan sonra yönetici yetkisine ulaşmaya çalışmasıdır. Bu şekilde yönetici yetkisiyle sistem üzerinde istedikleri bilgilere erişilebilir. DARPA veritabanında isimlendirildiği haliyle, en çok bilinen U2R saldırı tipleri Eject, Fbconfig, Fdformat, Loadmodule, Perl gibi saldırılardır[2].

2.3 Uzaktan Erişim (R2L)

Bu saldırı tipinde saldırgan saldırdığı makineye ağ üzerinden paketler yollayarak makinenin açıklarından yararlanmaya çalışmaktadır. Bu konuda birçok araç olması ve bu araçlara erişimin kolay olması sebebiyle, sistemde var olan açıklar saldırgandan önce tespit edilip kapatılmamışsa, oldukça etkili ve kolay bir saldırı yöntemidir. DARPA veritabanında

isimlendirildiği haliyle, en çok bilinen R2L saldırı tipleri Dictionary, Guest, Imap, Named, Sendmail gibi saldırılardır [2].

2.4 Yoklama (Probe)

Probe ya da Probing saldırısı olarak da bilinen yoklama saldırısı, ağı veya bilgisayarı tarayarak zayıflıkları tespit etmek ve sistem yapısı ile ilgili genel bir bilgiye ulaşmak için yapılmaktadır. Sistem hakkında detaylı bilgi edinildikten sonra nasıl bir saldırı yapılması gerektiği belirlenmektedir. Yoklama saldırısı için kullanılan araçlar aynı zamanda güvenlik uzmanları tarafından sistemin güvenliğinin test edilmesi için de kullanılan araçlardandır. DARPA veritabanında isimlendirildiği haliyle, en çok bilinen Probe saldırı tipleri, Ipsweep, Mscan, Nmap, Saint, Satan gibi saldırılardır [2].

3. Yöntem

Bu çalışmada KDD'99 veri kümesinin bir parçası olan %10'luk etiketli veri kümesi kullanılmıştır. KDD'99 veri kümesinin %10'luk etiketlenmiş kısmı ele alınarak sayısallaştırılmıştır eğitim için ele alınan tüm saldırılardan örneklemeler oluşturulmuştur. Bu örneklemelerden rastgele seçilerek meydana getirilen 3000 örnekli saldırı dosyası ve 2781 örnekli saldırı dosyaları kullanılmıştır. Test verisi olarak ise, rastgele seçilmiş 200 örnekli ve 222 örnekli saldırı dosyaları kullanılmıştır. Veri kümeleri YSA' ya doğrudan eğitme ve tek tek eğitime yöntemiyle bilinen ve bilinmeyen saldırı dosyaları ile dört farklı örnek saldırı dosyası şeklinde verilmiştir. Başarımlarının analizini yapmak için saldırı dosyaları ve test verileri MATLAB ile işlenerek mevcut sistemin bu saldırıları tanıyabilmesi ya da ayırt edebilmesi gözlenmiştir.[10]

Tablo 2. Çalışmada kullanılacak saldırı veri kümeleri

Kullanılan Yöntem	Bilinen	Bilinmeyen
Doğrudan Eğitim	**Örnek-1**	**Örnek-2**
	atak3000. txt	atak2781. txt
	ornek200. txt	ornek222. txt
Ayrı Eğitim	**Örnek-3**	**Örnek-4**
	ornek200. txt	ornek222. txt
	normal0. txt	normal0. txt
	Imap5. txt	Imap5. txt
	pod14. txt	pod14. txt

Çalışmada kullandığımız YSA yapısında, çok katmanlı algılayıcılı (ÇKA) ağ ve fonksiyon olarak YSA'larda hiperbolik tanjant fonksiyonu (tansig) aktivasyon fonksiyonu olarak kullanılmıştır. Tansig fonksiyonu türevi alınabilir, sürekli ve doğrusal olmayan bir fonksiyon olması nedeni ile doğrusal olmayan problemlerin çözümünde yaygın olarak kullanılmaktadır.

3.1 Tespit Edilecek Saldırılar

Çalışmada YSA'nın eğitiminde iki adet DoS saldırısının bulunduğu eğitim kümesi kullanılmıştır. Bu eğitim seti içerisinde Imap ve Pod saldırıları bulunmaktadır. Test

kümelerinde ise bilinmeyen saldırı tespitinde yoklama (probe) saldırısı kapsamında NMAP saldırısı kullanılmıştır.

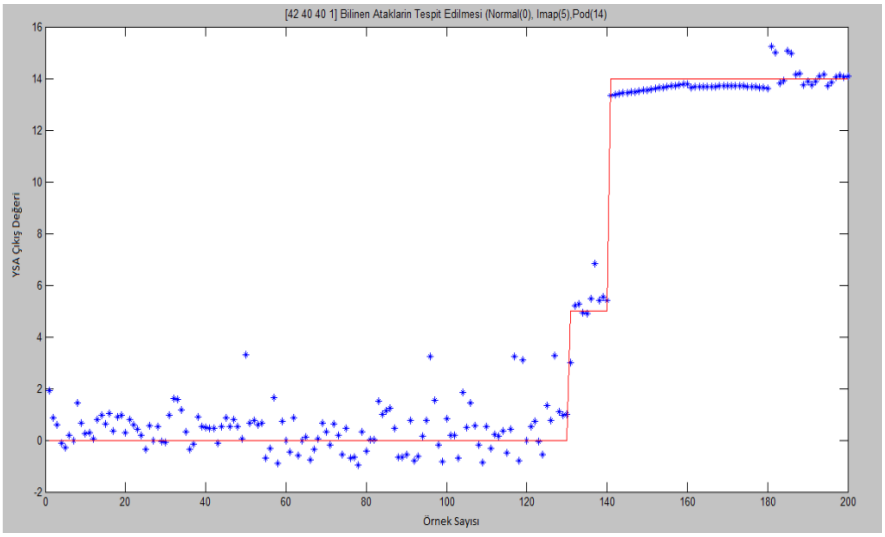
Çalışmada, normal atak 0,Imap=5,Pod=14 olarak sayısallaştırılmış ve YSA çıkışında bu değerlere yakınsaması beklenmektedir.

4. Saldırının Tespit Edilmesi ve Başarımları

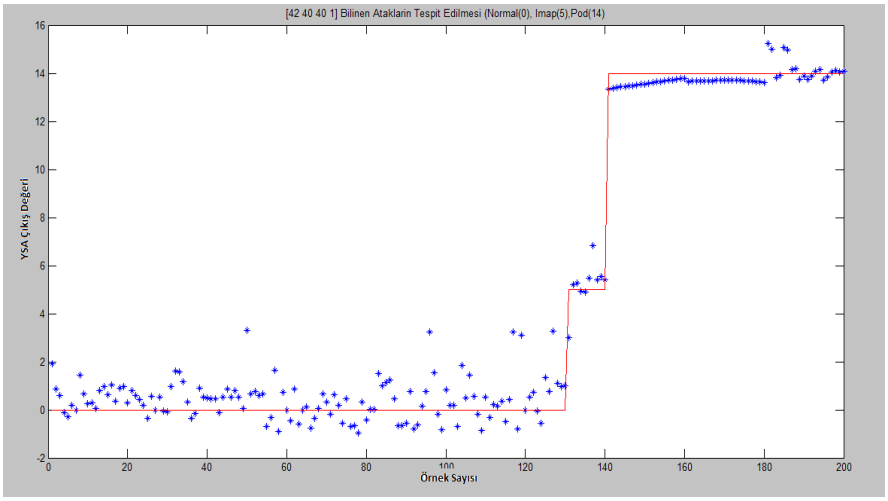
Bir bilişim sistemine karşı gerçekleştirilen saldırının tespitinde, öncelikle bilinen saldırı tipleri ile karşılaştırma yapılır. Bu karşılaştırma sonucu bir tespit yapılamaması durumunda bilinmeyen saldırı tipleri ile karşılaştırma yapılır.

4.1 Bilinen saldırının tespit edilmesi

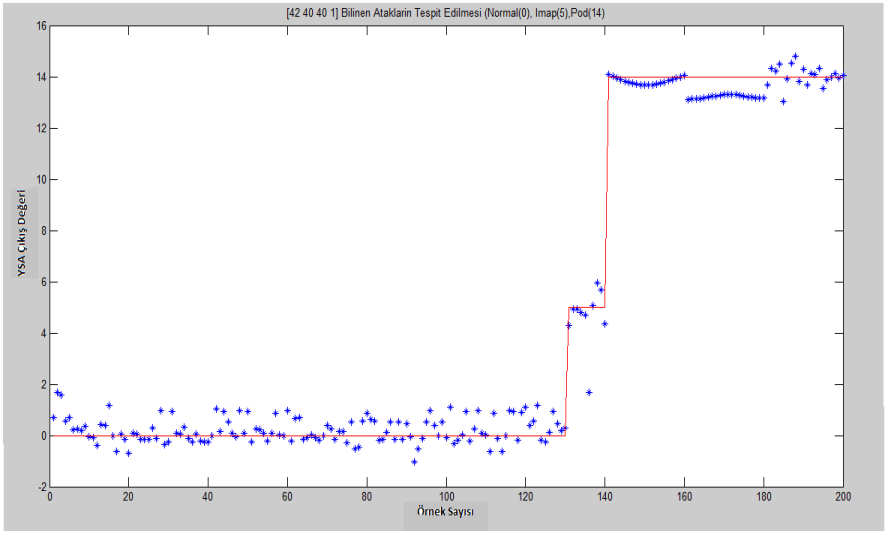
Bilinen saldırının tespit edilmesinde, ilk olarak eğitim setini doğrudan eğiterek, test verisindeki saldırı dosyalarını tespit etme işlemi gerçekleştirilmelidir. Bu amaçla gerçekleştirilenler Şekil 2,3 ve 4'de verilmiştir.



Şekil 2. Örnek-1 Bilinen Atakların Tespiti Deneme-1.



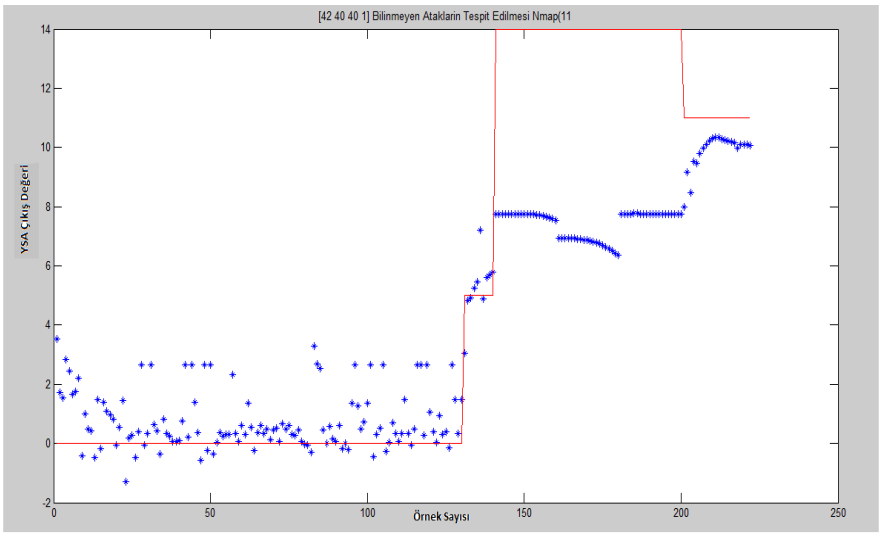
Şekil 3.Örnek-1 Bilinen Atakların Tespiti Deneme-2.



Şekil 4.Örnek-1 Bilinen Atakların Tespiti Deneme-3.

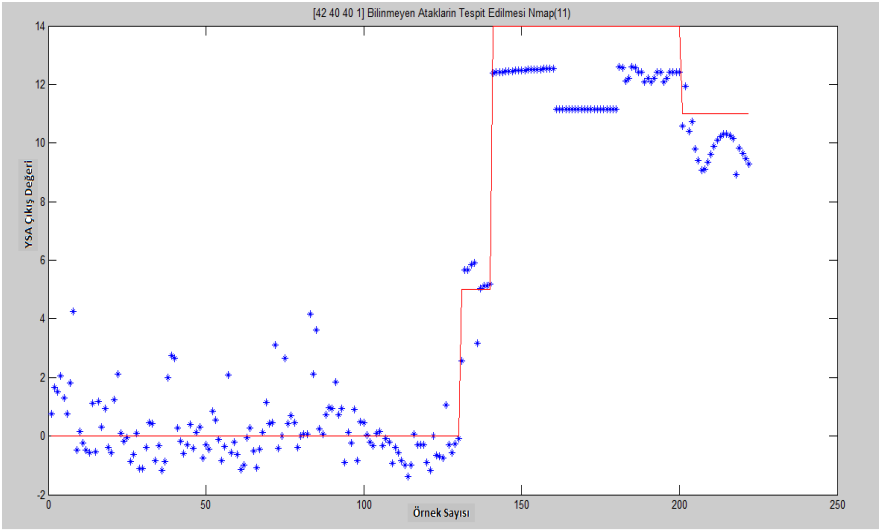
4.2 Bilinmeyen Saldırıların Tespit Edilmesi

Çalışmamızda bilinmeyen saldırının tespit edilmesi ilk önce içinde bulunması istenen (saldırı verisi çıkartılan) eğitim setini doğrudan eğitmek yöntemiyle test verisindeki saldırı dosyalarını tespit etmesi beklenmektedir. Yapılan denemeler aşağıda sırasıyla verilmiştir.



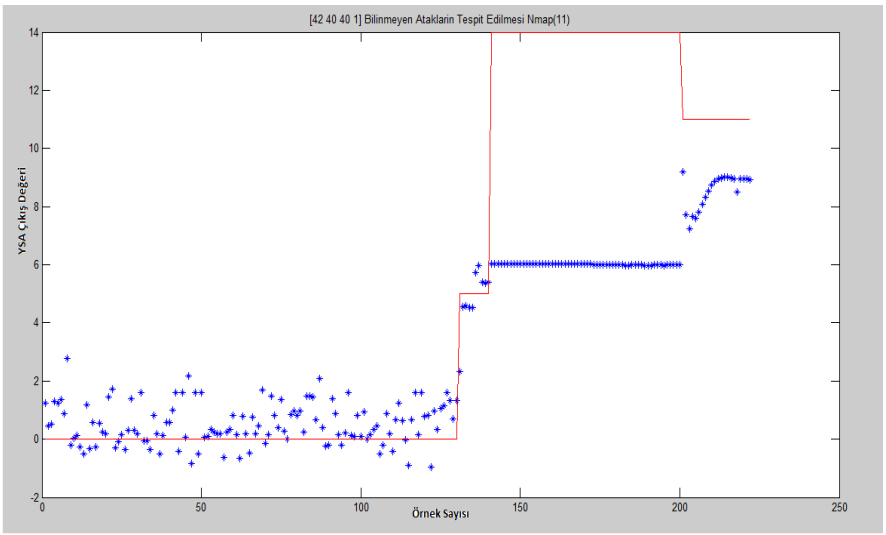
Şekil 5.Örnek-2 Bilinmeyen Atakların Tespiti-Deneme-1

Şekil 5'de Normal (0) saldırısı 0 ile 3 arasında değerler alsa da kendi değerine çoğunlukla yakınsamıştır. Imap (5) kendi değerlerine yakınsadığı Pod (14) saldırılarının kendi değerine yakınsamadığını, bilinmeyen saldırının 6-8 ve 10 değerlerine yakınsadığını gözlenmiştir.



Şekil 6.Örnek-2 Bilinmeyen Atakların Tespiti-Deneme-2.

Şekil 6'da Normal (0) saldırısı 0 ile 3 arasında değerler alsa da kendi değerine çoğunlukla yakınsamıştır. Imap (5) kendi değerlerine yakınsadığı Podl (14) saldırılarının kendi değerine yakınsamadığını fakat iki ayrı blok halinde 11 ve13 değerlerine yakınsadığı, bilinmeyen saldırının 9 ile 11 değerleri arasında değerler aldığını gözlenmiştir.



Şekil 7.Örnek-2 Bilinmeyen Atakların Tespiti-Deneme-3.

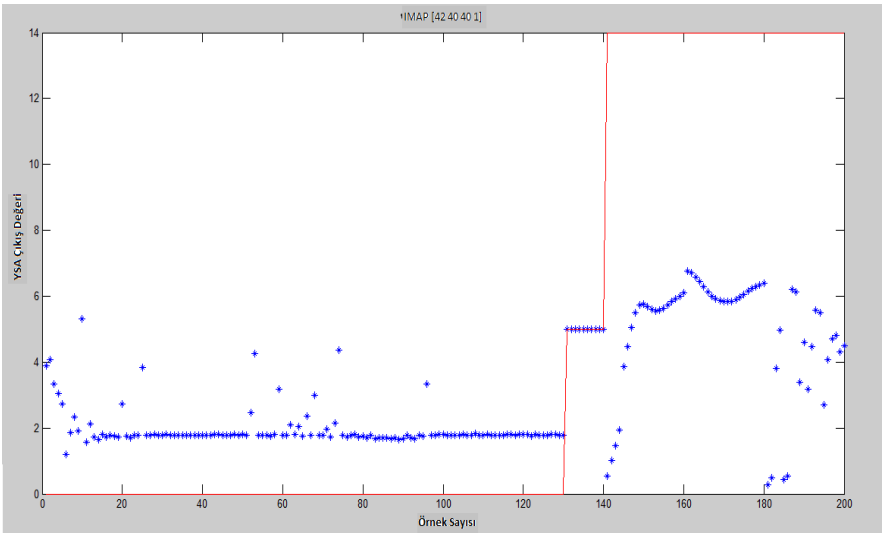
Şekil 7'de Normal (0) saldırısı 0 ile 2 arasında değerler alsa da kendi değerine çoğunlukla yakınsamıştır. Imap (5) 4ile 6 arasında değerler almıştır. Podl (14) saldırılarının kendi değerine yakınsamadığını blok halinde 6 değerlerine yakınsadığı, bilinmeyen saldırının 7 ile 9 değerleri arasında değerler aldığını göstermiştir. Tablo 3'de bilinmeyen atakların tespiti için yazılan kaba kod verilmiştir.

Tablo 3.Bilinmeyen Atakların Tespiti-Kaba Kodları.

```
%Bilinmeyen ataklarin bulunmasi
load ornek222. txt;  % Test Veri Seti yüklenmesi
load atak2781. txt;  % Nmap hariç tüm atakların olduğu veri setinin
yüklenmesi
P1,T1=atak 2781 atak dosyasının ÇKA tanıtılması
a1,s1=ornek222 ornek veri setinin ÇKA tanıtılması
net1= atak 2781 dosyası için YSA oluşturulması
net1. trainParam.epochs  % iterasyon parametresinin belirlenmesi
net1=YSA nın eğitilmesinin yapılması
y1=sim (YSA nın benzetimin yapılması);
figure;  %Grafiğin çizdirilmesi
plot (y1, '*');
hold
plot (s1', 'r');
title ('[42 40 40 1] Bilinen Ataklarin Tespit Edilmesi (Normal (0),
Imap (5), Pod (14)');  %Gafik başlığının yazılması
hold
```

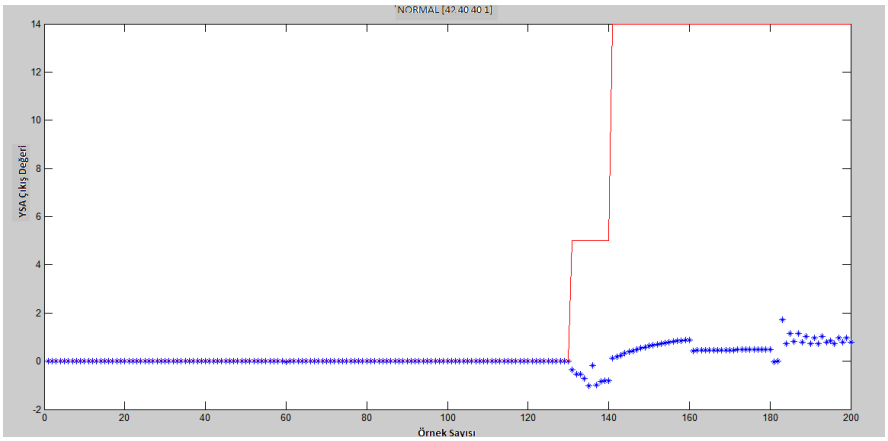
4.3 Ayrı Eğitim Yoluyla Saldırıların Tespit Edilmesi

Çalışmada saldırı veri kümeleri ayrı ayrı eğitilerek test verisindeki saldırı kümelerini yakalaması beklenmektedir. Elde edilen grafikler sırasıyla aşağıda gösterilmektedir.



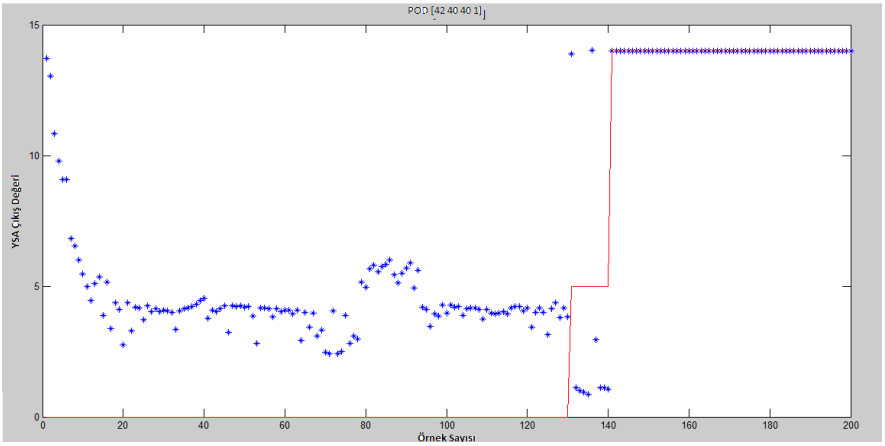
Şekil 8. Örnek-3 Ayrı Eğitim Setleri Bilinen Atakların Tespiti-Deneme-1-IMAP.

Şekil 8' de ayrı eğitim saldırı kümesinden normal (0) 2 değerine yakınsamış, Pod (14) 6 ile 8 değerleri arasında değişik değerler almış ve saldırıyı tanımamıştır fakat Imap (5) kendi değerini yakalamış ve saldırıyı tespit etmiştir.



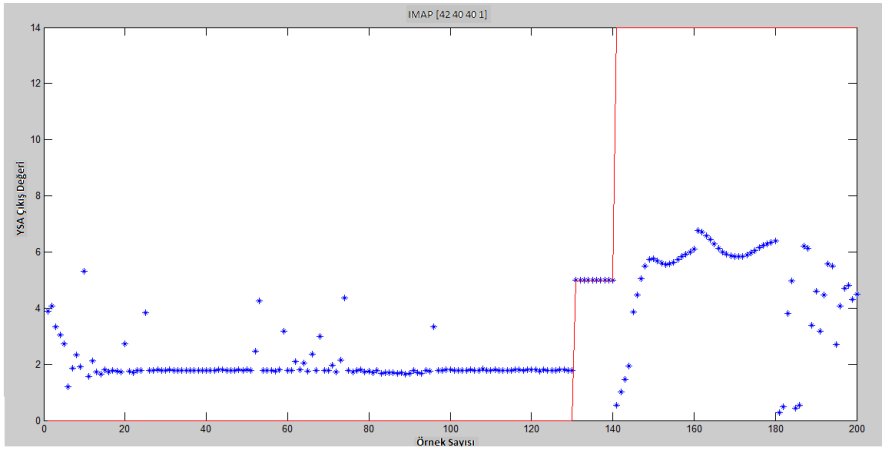
Şekil 9.Örnek-3 Ayrı Eğitim Setleri Bilinen Atakların Tespiti-Deneme-1-NORMAL.

Şekil 9'da ayrı eğitim saldırı kümesinden normal (0) kendi değerini yakalamış ve saldırıyı tespit etmiştir. Pod (14) ve Imap (5) saldırıyı tanımamıştır ve sıfıra yakınsamışlardır.



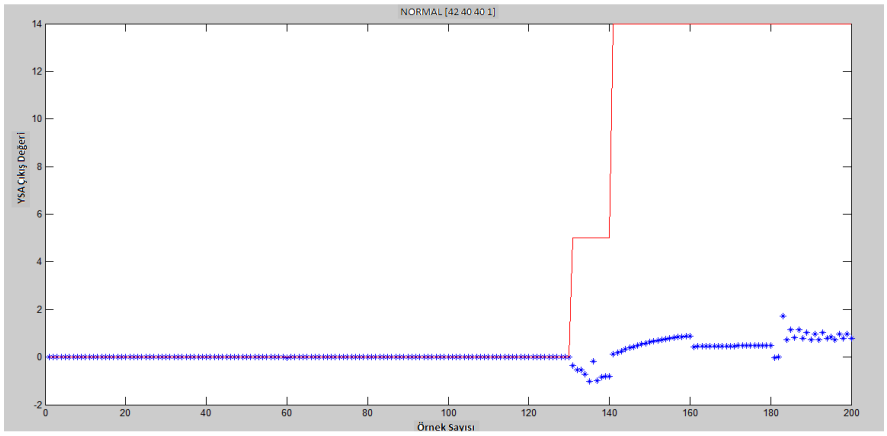
Şekil 10.Örnek-3 Ayrı Eğitim Setleri Bilinen Atakların Tespiti-Deneme-1-POD.

Şekil 10'da ayrı eğitim saldırı kümesinden Pod (14) kendi değerini yakalamış ve saldırıyı tespit etmiştir. Normal (0) ve Imap (5) saldırıyı tanımamıştır.



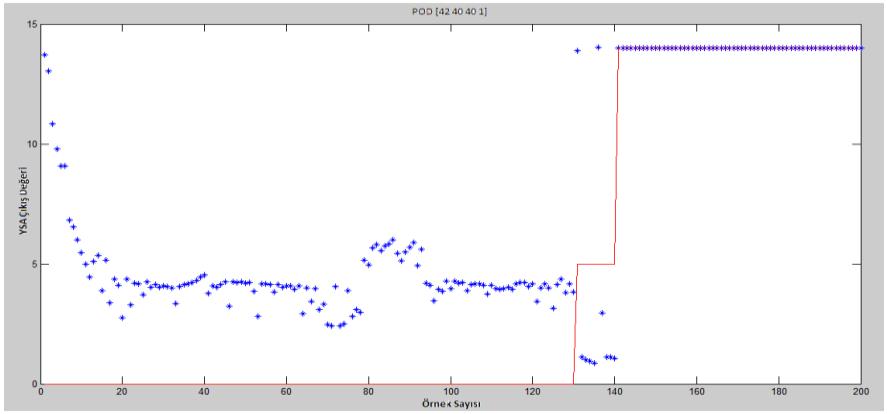
Şekil 11.Örnek-3 Ayrı Eğitim Setleri Bilinen Atakların Tespiti-Deneme-2-IMAP.

Şekil 11'de Imap (5) saldırı veri kümesi kendi değerini yakalamış ve saldırıyı tespit etmiştir.



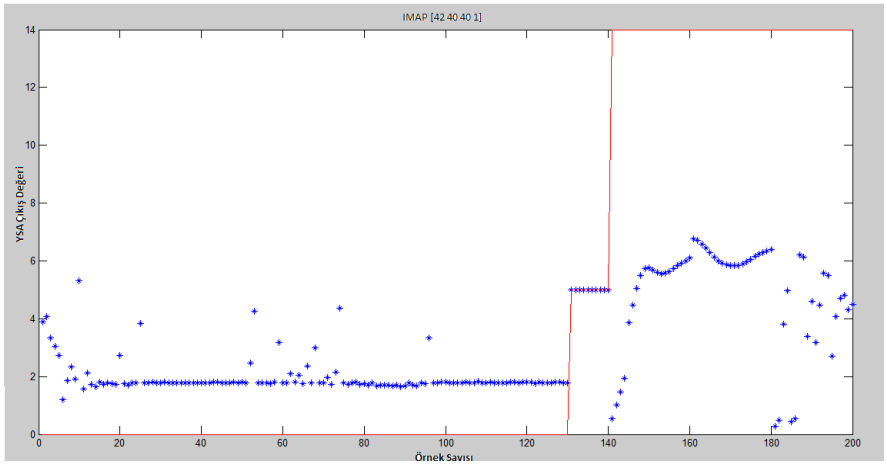
Şekil 12. Örnek-3 Ayrı Eğitim Setleri Bilinen Atakların Tespiti-Deneme-2-NORMAL.

Şekil 12'de Normal (0) saldırı veri kümesi kendi değerini yakalamış ve saldırıyı tespit etmiştir.

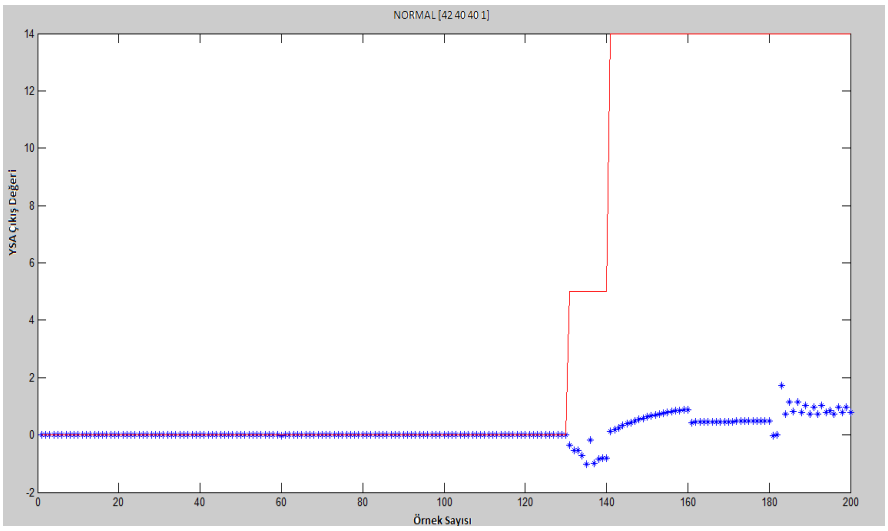


Şekil 13. Örnek-3 Ayrı Eğitim Setleri Bilinen Atakların Tespiti-Deneme-2-POD.

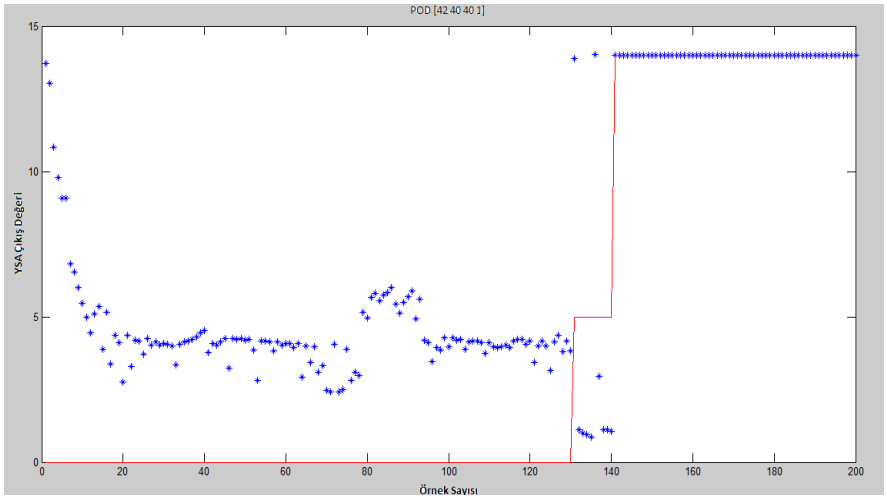
Şekil 13'de Pod (14) saldırı veri kümesi kendi değerini yakalamış ve saldırıyı tespit etmiştir.



Şekil 14.Örnek-3 Ayrı Eğitim Setleri Bilinen Atakların Tespiti-Deneme-3-IMAP.



Şekil 15. Örnek-3 Ayrı Eğitim Setleri Bilinen Atakların Tespiti-Deneme-3-NORMAL.



Şekil 16. Örnek-3 Ayrı Eğitim Setleri Bilinen Atakların Tespiti-Deneme-3-POD.

Şekil 14'de Imap (5), Şekil 15'de Normal (0) ve Şekil 16'da Pod (14) saldırı veri kümesi kendi değerini yakalamış ve saldırıyı tespit etmiştir.

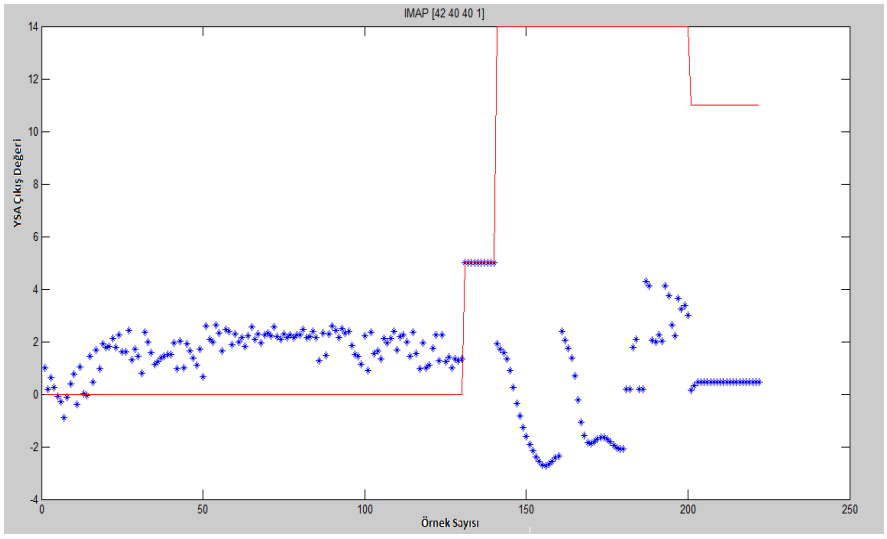
Tablo 4' de ayrı eğitim ile bilinen atakların tespiti için kaba kodları verilmiştir.

Tablo 4. Ayrı Eğitim-Bilinen Atakların Tespiti-Kaba Kodları.

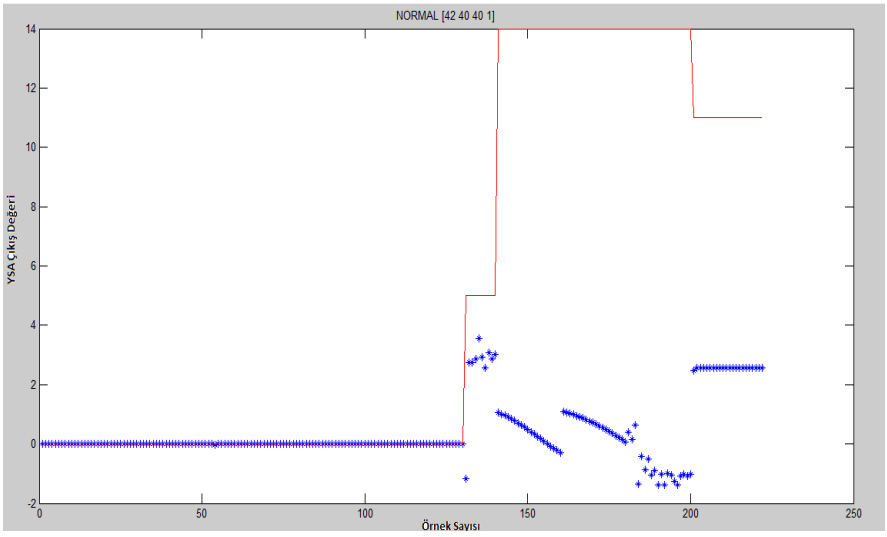
%Ayri Ayri Egitim

load ornek200. txt; %% Test Veri Seti Yüklenmesi
load normal0. txt; %% Normal Trafik Eğitim Seti Yüklenmesi
load Imap. txt; %% Imap Atağı Veri DosyasınınYüklenmesi
load pod. txt; %% Pod Atağı Veri DosyasınınYüklenmesi
P1,T1 =normal0 atağın ÇKA ya tanıtılması
P2,T2=Imap5 atağın ÇKA ya tanıtılması
P3,T3=pod14 atağın YSA ya tanıtılması
a1,s1=ornek200 test veri setinin tanıtılması
net1= Normal0 atağı için YSA eğitiminin yapılması

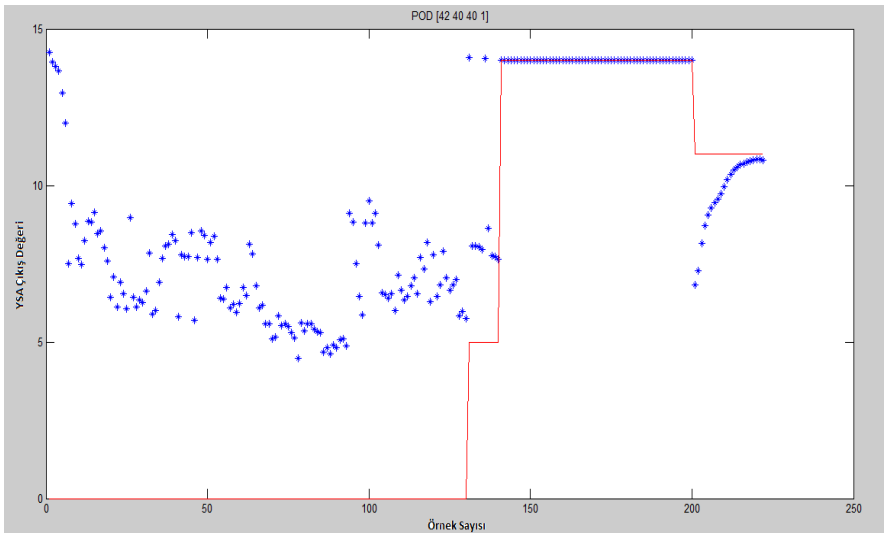
```
net2= Imap5 atağı için YSA eğitiminin yapılması
net3= Pod14 atağı için YSA eğitiminin yapılması
net1. trainParam. Epochs % iterasyon parametresinin belirlenmesi
net2. trainParam. Epochs % iterasyon parametresinin belirlenmesi
net3. trainParam. Epochs% iterasyon parametresinin belirlenmesi
y1=sim (net1 ağının benzetimi yapılması);
y2=sim (net2 ağının benzetimi yapılması);
y3=sim (net3 ağının benzetimi yapılması);
figure;plot (y1, '*'); %Grafiklerin ayrı ayrı çizdirilmesi
hold
plot (s1', 'r');title (' NORMAL [41 40 40 1] '); figure; plot (y2, '*');
hold
plot (s1', 'r');title (' IMAP [41 40 40 1] '); figure; plot (y3, '*');
hold
plot (s1', 'r');title (' POD [41 40 40 1]');
hold
```



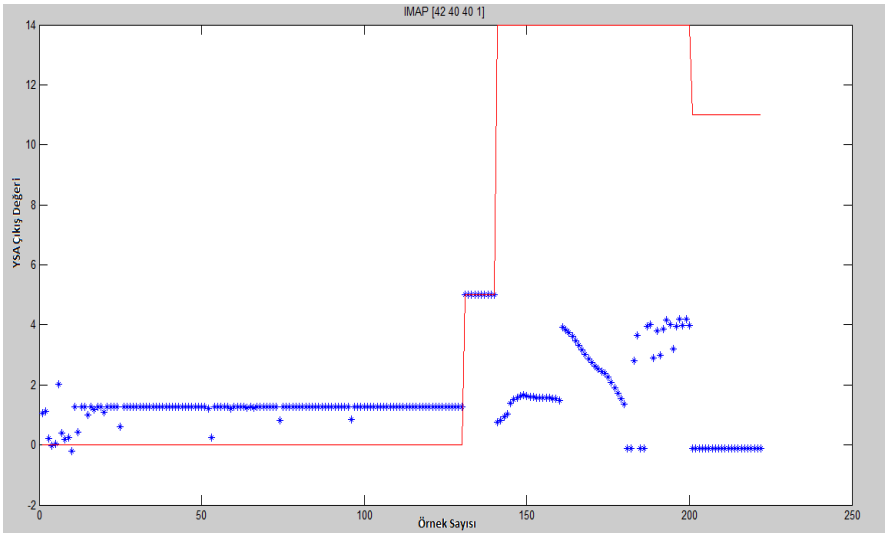
Şekil 17. Örnek-4 Ayrı Eğitim Setleri Bilinmeyen Atakların Tespiti-Deneme-1-IMAP.



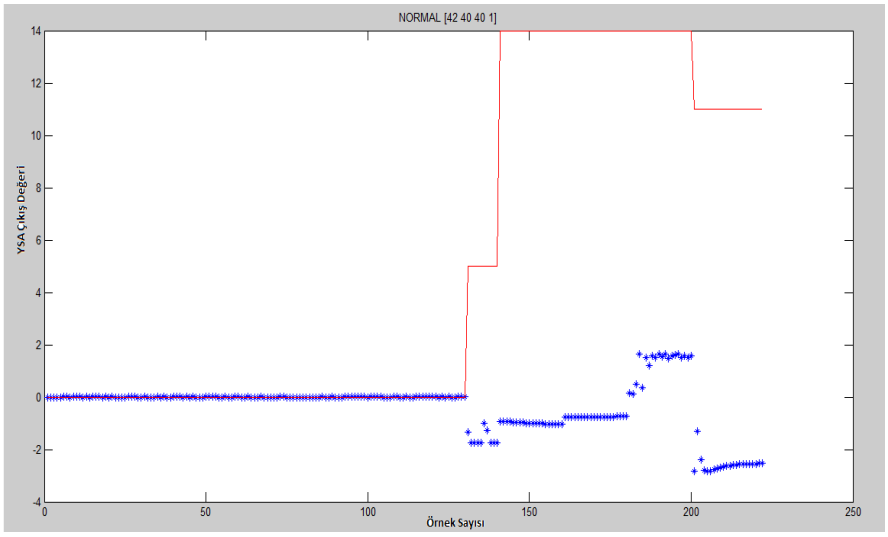
Şekil 18. Örnek-4 Ayrı Eğitim Setleri Bilinmeyen Atakların Tespiti-Deneme-1-NORMAL.



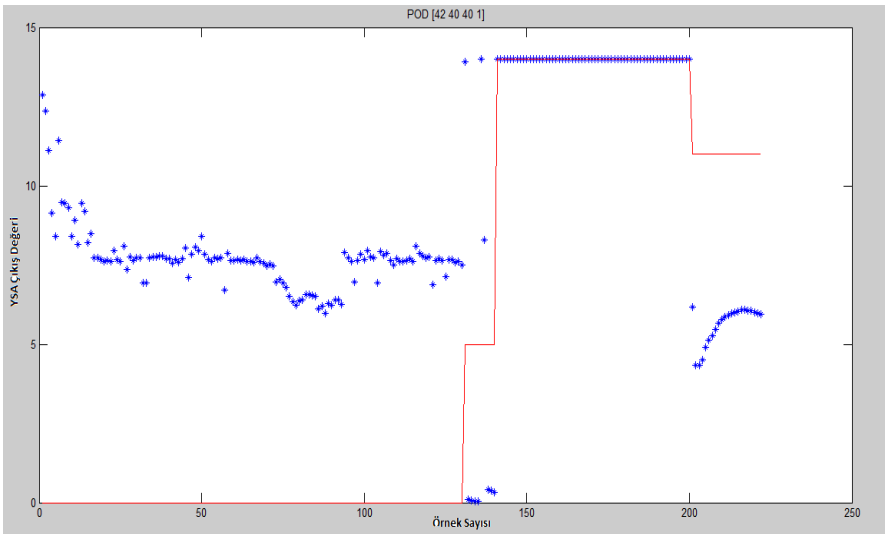
Şekil 19. Örnek-4 Ayrı Eğitim Setleri Bilinmeyen Atakların Tespiti-Deneme-1-POD.



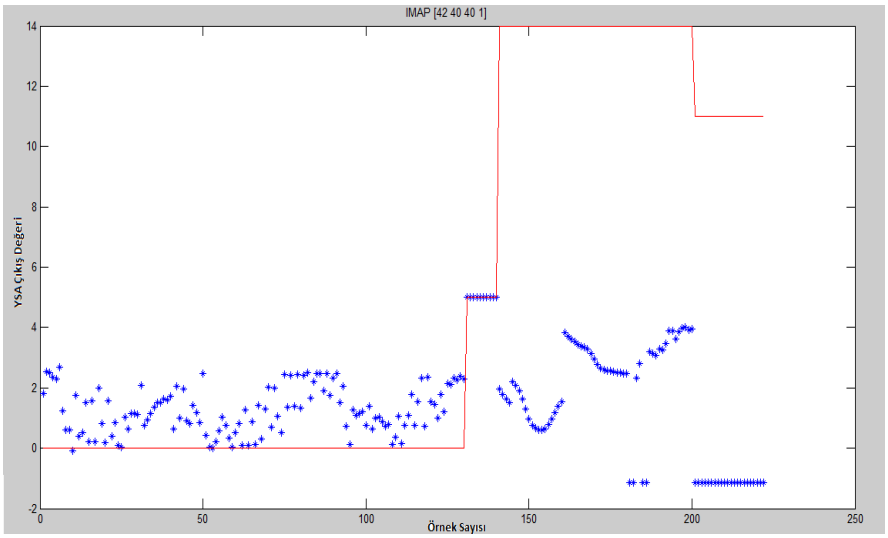
Şekil 20. Örnek-4 Ayrı Eğitim Setleri Bilinmeyen Atakların Tespiti-Deneme-2-IMAP



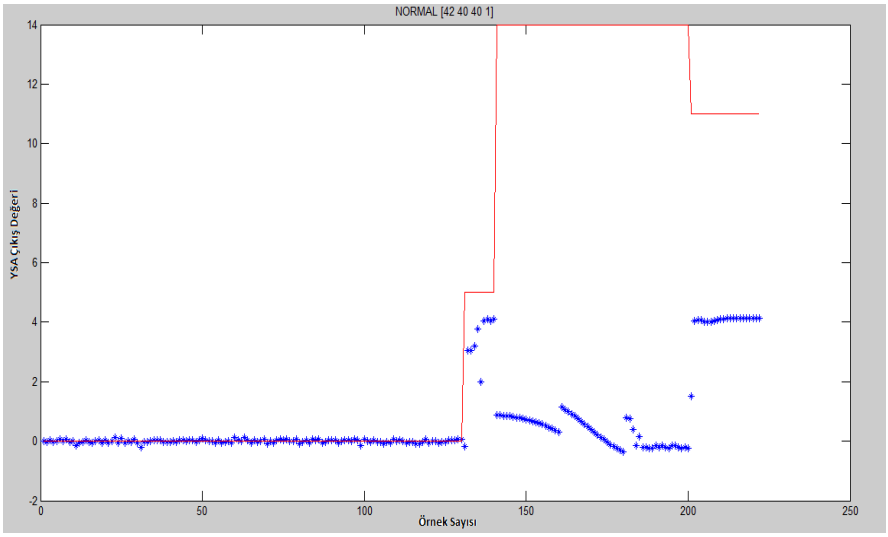
Şekil 21. Örnek-4 Ayrı Eğitim Setleri Bilinmeyen Atakların Tespiti-Deneme-2-NORMAL



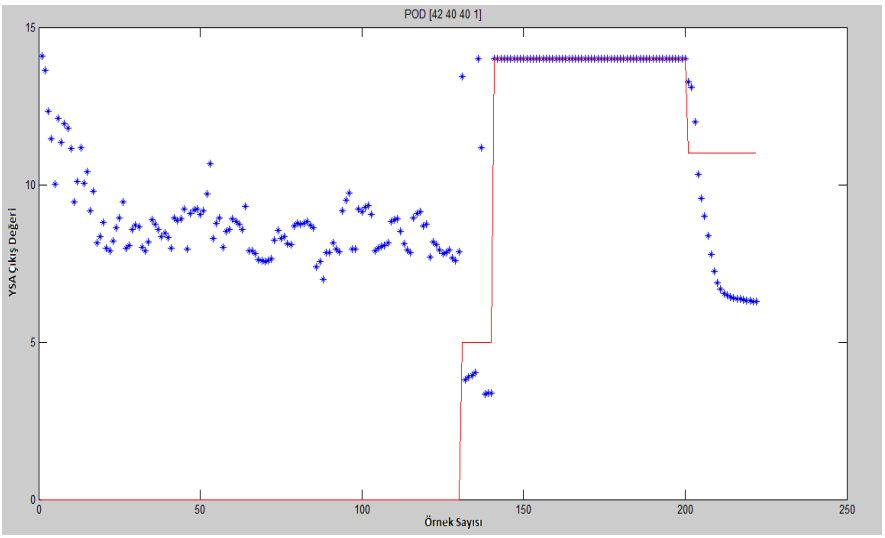
Şekil 22. Örnek-4 Ayrı Eğitim Setleri Bilinmeyen Atakların Tespiti-Deneme-2-POD.



Şekil 23. Örnek-4 Ayrı Eğitim Setleri Bilinmeyen Atakların Tespiti-Deneme-3-IMAP.



Şekil 24. Örnek-4 Ayrı Eğitim Setleri Bilinmeyen Atakların Tespiti-Deneme-3-NORMAL.



Şekil 25. Örnek-4 Ayrı Eğitim Setleri Bilinmeyen Atakların Tespiti-Deneme-3-POD.

5. Saldırı Başarımlarının Tespit Edilmesi

Çalışmada saldırı tespitinin test edilmesinde başarım oranlarının tespitinde aşağıdaki denklem kullanılmıştır. Bu denklem Tanrıkulu[8]'nun çalışmasında da kullanılmıştır. Denklemde yakınsayacak değer saldırı tespitinde sayısallaştırdığımız saldırı tespit sıra numaralarıdır. Ortalama ise YSA 'nın yapılan testler için denemelerin çıktı değerlerinin aritmetik ortalamasıdır. Örneğin, Imap saldırısı için yd=5 olması beklenir. Çıktı değerlerinin ortalaması ise ort=4.5 çıkmış olabilir. Eşitlikte değerler yerine yazılarak elde edilen sonuçlar başarım oranlarını vermektedir.

$$SBB = \frac{yd \quad |yd \quad ort|*100}{yd} \tag{1}$$

SBB= Saldırı bulma başarımı (%),
yd=Yakınsanması istenen değer,
ort=YSA çıktı değerlerinin aritmetik ortalamasını göstermektedir.

5.1 Normal Saldırı Verisinin Başarımını Tespit Edilmesi

Denklemde yakınsanacak değer saldırı tespitinde sayısallaştırdığımız saldırı tespit sıra numaralarıdır. Ortalama ise YSA 'nın yapılan testler için denemelerin çıktı değerlerinin aritmetik ortalamasıdır. Diğer saldırılardan farklı olarak Normal saldırı değeri 0 (sıfır) sayısal değeri verildiği için YSA çıkışları -1 ve 1 arasındaki sıfır değerine yakınsayacaktır. Diğer saldırı bulma başarım denklemi sıfır değerine bölmek anlamsız olacağından Denklem 2 kullanılmıştır. Denklemde değerler yerine yazılarak elde edilen sonuçlar başarım oranlarını vermektedir.

$$NSBB = |1 - ort|*100 \tag{2}$$

Denklemde;
NSBB= Normal saldırıyı bulma başarımı (%),
yd=Yakınsanması istenen değer,
ort=YSA çıktı değerlerinin aritmetik ortalamasını göstermektedir.

6. Sonuç

Yapılan çalışma kapsamında veriler 2 farklı yöntem 4 ayrı örnek ve her birindeki 3 farklı deneme için elde edilen veriler çizelgelerde gösterildiği gibidir.

Tablo 5. Örnek-1 süre ve başarım bilgileri

Deney: Ornek-1 (Bilinen)				
Yöntem:Dogrudan Egitim				
YSA Yapısı: [42 40 40 1]				
Deneme-1				
Süre (sn)	Iterasyon	Basarım (%)		
		Normal (0)	Imap (5)	Pod (14)
492	19	56. 4138	96. 0634	98. 6488
Deneme-2				
Süre (sn)	Iterasyon	Basarım (%)		
		Normal (0)	Imap (5)	Pod (14)
1060	50	83. 7797	95. 7308	67. 8055
Deneme-3				
Süre (sn)	Iterasyon	Basarım (%)		
		Normal (0)	Imap (5)	Pod (14)
495	19	78. 5713	92. 6579	97. 8380

Yapılan "Örnek-1" deneyinde bilinen saldırı kümeleri için doğrunda eğitim yoluyla 3 ayrı deneme yapılmıştır. Deneyde amaç olarak eğitim kümesinin net. 1 YSA nın öğrenmesi sağlamaktır. Deney süreleri, iterasyon (yenileme) miktarı ve başarım yüzdeleri Tablo 5' de gösterilmiştir. "Örnek-1" deneyinde 3 ayrı saldırı sonucun ortalamaları sırasıyla Normal (0) için %72. 92, Imap (5) için %94. 81, Pod (14) için %88.09 olarak bulunmuştur. "Örnek-1" deneyinde eğitilen saldırı veri dosyasının (atak3000. txt) sonucu test verinde (ornek200) bulunan saldırıları yakaladığı anlaşılmıştır.

Tablo 6.Örnek-2 süre ve başarım bilgileri

Deney: Ornek-2 (Bilinmeyen)					
Yöntem:Dogrudan Egitim					
YSA Yapısı: [42 40 40 1]					
Deneme-1					
Süre (sn)	Iterasyon	Basarım (%)			
		Normal (0)	Imap (5)	Pod (14)	Nmap (11)
489	21	93, 707	96, 4423	99, 9237	28, 0639
Deneme-2					
Süre (sn)	Iterasyon	Basarım (%)			
		Normal (0)	Imap (5)	Pod (14)	Nmap (11)
1104	50	72, 8587	99, 2002	96, 0477	27, 7629
Deneme-3					
Süre (sn)	Iterasyon	Basarım (%)			
		Normal (0)	Imap (5)	Pod (14)	Nmap (11)
422	18	73, 5434	61, 4515	69, 9791	23, 151

Yapılan "Örnek-2" deneyinde bilinmeyen saldırı kümeleri için doğrudan eğitim yoluyla 3 ayrı deneme yapılmıştır. Deneyde amaç olarak eğitim kümesinde olmayan bir saldırı olan Nmap (11) saldırısını net. 1 YSA nın öğrenmesi ve yakalaması hedeflenmiştir. Deney süreleri, iterasyon (yenileme) miktarı ve başarım yüzdeleri Tablo 6' da gösterilmiştir. "Örnek-2" deneyinde 3 ayrı saldırı sonucun ortalamaları sırasıyla Normal (0) için %80. 03, Imap (5) için %85. 69, Pod (14) için %88. 65 ve Nmap (11) için ise %26. 32 olarak tespit ettiği görülmüştür. "Örnek-2" deneyinde eğitilen saldırı veri dosyasının (atak2781. txt) sonucu test verinde (ornek222. txt) bulunan saldırılardan Normal (0), Imap (5) ve Pod (14) saldırılarını yüksek yüzdelik oranlarında yakaladığı fakat bilinmeyen saldırı olarak Nmap (11) saldırısını düşük yüzdelik oranıyla yakaladığı gözlenmiştir.

Tablo 7.Örnek-3 süre ve başarım bilgileri

Deney: Ornek-3 (Bilinen)				
Yöntem:Ayrı Egitim				
YSA Yapısı: [42 40 40 1]				
Deneme-1				
Süre (sn)	Iterasyon	Basarım (%)		
		Normal (0)	Imap (5)	Pod (14)
1125	50	99, 9835	99, 9954	99, 9956
Deneme-2				
Süre (sn)	Iterasyon	Basarım (%)		
		Normal (0)	Imap (5)	Pod (14)
1062	50	99, 9835	99, 9954	99, 9956
Deneme-3				
Süre (sn)	Iterasyon	Basarım (%)		
		Normal (0)	Imap (5)	Pod (14)
973	45	99, 9835	99, 9954	99, 9956

Yapılan "Örnek-3" deneyinde bilinen saldırı kümeleri için ayrı eğitim yoluyla 3 ayrı deneme yapılmıştır. Deneyde amaç olarak eğitim kümesinde yakalanması istenilen saldırı veri kümeleri teker teker ve ayrı olarak eğitilerek net1, net2, net3 YSA ağlarına öğretmek ve bulunmasını sağlamaktır. Deney süreleri, iterasyon (yenileme) miktarı ve başarım yüzdeleri 7' de gösterilmiştir. "Örnek-3" deneyinde 3 ayrı saldırı veri kümesi için farklı süreler ve iterasyon (yenileme) miktarları çıkmasına rağmen aynı sonuçlar elde edilmiştir. Sonuçların ortalamaları sırasıyla Normal (0) için %99. 98, Imap (5) için %99. 99, Pod (14) için %99. 99 oranlarında tespit edildiği görülmüştür. Örnek-3 deneyinde eğitilen saldırı veri dosyaları normal0. txt, Imap5. txt, pod14. txt sonucu test verinde (ornek200. txt) bulunan saldırılardan Normal (0), Imap (5) ve Pod (14) saldırılarını yüksek yüzdelik oranlarında yakaladığı ve tanıdığı gözlenmiştir.

Tablo 8. Örnek-4 süre ve başarım bilgileri

Deney: Ornek-4 (Bilinmeyen)					
Yöntem:Ayrı Egitim					
YSA Yapısı: [42 40 40 1]					
Deneme-1					
Süre (sn)	Iterasyon	Basarım (%)			
		Normal (0)	Imap (5)	Pod (14)	Nmap (11)
540	10	99, 9999	99, 9962	99, 9929	0

Deneme-2					
Süre (sn)	Iterasyon	Basarım (%)			
		Normal (0)	Imap (5)	Pod (14)	Nmap (11)
780	8	99, 9597	99, 9859	99, 9926	0
Deneme-3					
Süre (sn)	Iterasyon	Basarım (%)			
		Normal (0)	Imap (5)	Pod (14)	Nmap (11)
780	8	99, 8733	99, 9908	99, 9965	0

Yapılan "Örnek-4" deneyinde bilinmeyen saldırı kümeleri için ayrı eğitim yoluyla 3 ayrı deneme yapılmıştır. Deneyde amaç olarak eğitim kümesinde yakalanması istenilen saldırı veri kümeleri teker teker ve ayrı olarak eğitilerek net1, net2, net3 YSA ağlarına öğretmek ve bulunmasını sağlamaktır. Deney süreleri, iterasyon (yenileme) miktarı ve başarım yüzdeleri Tablo 8' de gösterilmiştir. "Örnek-4" deneyinde 3 ayrı saldırı veri kümesi için elde edilen sonuçların ortalamaları sırasıyla Normal (0) için %99. 99, Imap (5) için %99. 94, Pod (14) için %99. 99 ve Nmap (11) için ise %0 oranlarında tespit edildiği görülmüştür. Örnek-4 deneyinde eğitilen saldırı veri dosyaları normal0. txt, Imap5. txt, pod14. txt sonucu test verinde (ornek222. txt) bulunan saldırılardan Normal (0), Imap (5) ve Pod (14) saldırılarını yüksek yüzdelik oranlarında yakaladığı ve tanıdığı gözlenmiştir. Bilinmeyen ve bulunması istenilen Nmap (11) saldırısını ise yakalayamadığı gözlenmiştir.

Tablo 9. Çalışmadaki Ortalama Başarım Oranları

YSA Yapısı	**İşlem Eleman Sayısı**	**Veri Seti**	**Özellik Sayısı**	**Bilinen Saldırıların Bulunması Ortalama Başarım Oranı (%)**	**Bilinmeyen Saldırıların Bulunması Ortalama Başarım Oranı (%)**
ÇKA	[42 40 40 1]	KDD'99	42	92, 6352	72, 5799

Yapılan çalışmada 2 farklı yöntem ile 4 farklı örnek 12 deneme sonucu oluşturulan veri başarımlarını gösteren tablo yukardaki gösterildiği gibidir. Bilinen saldırının bulunmasındaki başarım oranı ortalaması %92,64 olarak saldırı tespitinin başarılı olduğunu gösterirken, bilinmeyen saldırının tespiti noktasında elde edilen oran %72, 58 olarak başarılı olduğunu göstermektedir.

Yapılan çalışmada YSA 'nın bir eğitim kümesi üzerinden sinir ağının tamamını öğrenmesinde başarılı olduğundan dolayı Normal (0) ile tüm saldırıları bilgilerinin tespitinde başarılı olmuştur. Sinir ağının tamamını öğrenen YSA yapısında ağırlık önce rastgele seçilse de karşılaştırmalı olarak ağırlıklar değiştirilmekte ve saldırı tespitinde ayırt edici olmaktadır. YSA aslında kendine öğretilen bir veriyi bulmaya çalışacaktır. Bunu yaparken ise farklı ağırlık değerleri, farklı süreler ve farklı yinelemeler (iterasyon) denemektedir. Mesela Imap (5) saldırısını öğrenen bir YSA test veri kümesi içinde Pod (14) ve Normal (0) saldırılarıları bir grup olarak algılarken Imap (5) saldırısını ayrı bir grup olarak tanımlayacaktır. Dolayısı ile sadece öğrendiği saldırıyı diğer gruplardan ayırabilme yeteneğine sahip olan bir YSA yapısı bilinmeyen bir saldırı kümesi ile karşılaştığında bu saldırıyı sadece kendisinden farklı olan gruba ait olduğunu tanımlayacaktır.

Sonuçta, YSA eğitimini aldığı saldırı kümesi dışında kalan tüm saldırıları ve normal trafiği tek bir değere yakınsama durumu göstermiştir. Bu nedenle yaptığımız örnekler ve denemelerde tek tek saldırıları öğrenen ağlar tüm saldırılar aynı değerlere yakınsama durumu göstermiştir. Tüm ağı öğrenen YSA'lar başarım oranları yüksek olması olumlu olarak görülürken ağın büyüklüğüne göre yinelemeler (iterasyon) öğrenme sürelerinin fazla olması olumsuz olarak deneylerimizde gözlenmiştir.

Logaritmik sigmoid aktivasyon fonksiyonları kullanan YSA'lar bilinen saldırıları yakalamada başarılı olmalarına rağmen bilinmeyen saldırıları yakalamada başarılı olmadıkları gözlenmiştir. [9] Altun [11] çalışmalarında belirttiği gibi hiperbolik tanjant sigmoid (tansig) ve doğrusal aktivasyon (purelin) fonksiyonlarını kullanarak eğitilen YSA'ların sınıflandırma problemlerinin çözümünde yüksek başarımlar elde ettiği bu çalışmada da gözlenmiştir.

Tablo 10. Çalışmanın ortalama başarım değeri

Marttin (2014)	ÇKA	[42 40 40 1]	KDD'99	42	83,11

Tablo 10'da yapılan çalışmanın bilinen ve bilinmeyen saldırılara göre ortalama başarımı verilmektedir.

Literatür bilgisinde verildiği üzere, yapılan çalışmalardan ÇKA,veri kümesi ve kullanılan özellik olarak Mukkamala [2] çalışmalarıyla karşılaştırıldığında Mukkamala'nın elde ettiği % 99,25'lik başarım oranın bulunmasında ÇKA / DVM'nin birlikte çalıştırılmasından kaynaklandığı görülmektedir.

İleriki çalışmalarda, özel amaçlı bir bilgisayar ya da sunucu ile yapıldığında iterasyon sürelerinin değişebileceği bilinmelidir (Çalışmanın yapıldığı bilgisayar, Intel i3-2.4GHz işlemci ile 3GB belleğe sahip ve işletim sistemi Windows-64 bit). Güncel saldırıları kullanarak benzer çalışma yapılabilir fakat güncel saldırılarının tespitinde veri setlerinin oluşturulması güç ve pahalı olduğundan gönüllülerin ya da ağ güvenlik şirketlerinin oluşturduğu kara listelerden (blacklist) temin edilip kullanılabilir.

7. Kaynaklar

[1] (http://www. ll. mit. edu/IST/ideval)

[2] Mukkamala, S. , Janoski, G. , Sung, A. , "Intrusion detection using neural networks and support vector machines", ***IEEE International Joint Conferenceon Neural Networks***, IEEE Computer Society Press, 1702-1707 (2002).

[3] Moradi, M. , Zulkernine, M. , "A neural network based sistem for intrusion detection and classification of attacks, " ***IEEE International Conference on Advances in Intelligent Sistems - Theory and Applications***, Luxembourg- Kirchberg, Luxembourg, 148:1-6 (2004).

[4] Güven, E. N, "Zeki Saldırı Tespit Sistemlerinin İncelenmesi, Tasarımı ve Gerçekleştirilmesi".Yüksek Lisans Tezi, ***Gazi Üniversitesi Fen Bilimleri Enstitüsü,*** Ankara, (2007).

[5] Erol, M. "Saldırı Tespit Sistemlerinde İstatistiksel Anormallik Belirleme Kullanımı".**İTÜ Bilgisayar Müh. Bölümü**, İstanbul (2005).

[6] Cannady J. , "Artificial neural networks for misuse detection", ***Proceedings of the 1998 National Information Systems Security Conference (NISSC'98),*** Arlington, VA, 443-456 (1998).

[7] Ryan, J. , Lin, M. J. , Mikkulainen, R. , "Intrusion Detection with Neural Networks",***Advances in Neural Information Processing sistems 10***, Cambridge, MA, MIT Press, 1-7 (1998).

[8] Tanrıkulu, H, "Saldırı Tespit Sistemlerinde Yapay Sinir Ağların Kullanılması", ***Yüksek Lisans Tezi, Ankara Üniversitesi Fen Bilimleri Enstitüsü,*** Ankara, (2009).

[9] Marttin, V," "Saldırı Tespit Sistemlerinde Yapay Sinir Ağlarının Kullanımı ve Başarımlarının İncelenmesi" ***Yüksek Lisans Tezi, Bilecik Şeyh Edebali Üniversitesi Fen Bilimleri Enstitüsü*** Bilecik, (2014).

[10] Knowledge Discoveri and Deliveri, "KDD Cup 1999: General Information", http://www. sigkdd. org/kddcup/index. php?section=1999&method =info (15.08.2015).

[11] Massachusetts Teknoloji Enstitüsü Lincoln Laboratuarları "Off-line intrusion detection evaluation data" http://www. ll. mit. edu/IST/ideval/ (15.08.2015).

[12] MIT, (Massachusetts Teknoloji Enstitüsü Lincoln Laboratuarları) **"1998 DARPA Intrusion Detection Evaluation Data Set Overview",**
http://www. ll. mit. edu/IST/ideval/data/1998/1998_data_index. html, (15.08.2015).

[13] MIT, (Massachusetts Teknoloji Enstitüsü Lincoln Laboratuarları) **"1999 DARPA Intrusion Detection Evaluation Data Set Overview",**
http://www. ll. mit. edu/IST/ideval/data/1999/1999_data_index. html, (15.08.2015).

[14] MIT, (Massachusetts Teknoloji Enstitüsü Lincoln Laboratuarları) **"2000 DARPA Intrusion Detection Evaluation Data Set Overview",**
http://www. ll. mit. edu/IST/ideval/data/2000/2000_data_index.html, (15.08.2015).