Ağ Kullanım Analizi ile Nüfuz Tespiti

Rahim Karabağ, Hidayet Takçı, İbrahim Soğukpınar

***Özet*— Ağ güvenliği denilince güvenlik duvarı dışında ilk akla gelen nüfuz tespit sistemleridir. Ticari veya ticari olmayan birçok nüfuz tespit sistemi geliştirilmiş olup bunların bir kısmı hala geliştirilmeye devam etmektedir. Bu çalışmada iç ağa ait verilerin analizi ile nüfuz tespit işlemi gerçekleştirilmeye çalışılmıştır. Sistem dört aşamadan oluşmaktadır. İlk aşamada ağdan veriler toplanmakta, ikinci aşamada verilere dayalı olarak kümeler oluşturulmakta ve her bir kullanıcı atandığı küme numarası ile etiketlenmekte, üçüncü aşamada ise test verileri üzerinde kullanıcıların küme değiştirip değiştirmediğinin analizi yapılmaktadır. Geliştirilen modelde DARPA 99 veri setine ait TCPdump verileri kullanılmıştır. Kullanıcıların küme dışına çıkıp çıkmadığını test için Matlab üzerinde kNN uygulaması geliştirilmiştir. Kullanıcının bulunduğu kümeden dışarı çıkması anormallik olarak tespit edilmiştir.**

***Anahtar kelimeler*—Ağ izleme, Anormallik, Bilgisayar ağ güvenliği, en yakın komşu, Nüfuz Tespit sistemleri, veri madenciliği**

I. GİRİŞ

İnternetin gelişmesi ve bilgiye erişimin kolaylaşmasıyla ağ güvenliği en üst seviyede önem kazanmıştır. Ağ güvenliği için birçok savunma sistemi geliştirilmiştir. Fakat buna rağmen güvenlik problemleri devam etmektedir. Yeni geliştirilen donanım ve yazılımlar güvenlik açıklıklarını da beraberinde getirmiştir. Ağda kullanılan savunma sistemleri; genellikle dış ağdan koruma için kullanılan güvenlik duvarı ve iç ağda çalışan nüfuz tespit sistemleridir. Herhangi bir cihaz, sistem veya kullanıcı ağa dahil olduğu andan itibaren bilinçli veya bilinçsiz bir saldırgan olma ihtimali olacaktır. Bu durum, savunma sistemlerinin ağ içerisindeki her bir sistemi kontrol altında tutmasını gerektirmektedir. Bu işlem için ağ verileri bir merkezden toparlanmalı ve gerekli analizler yapılmalıdır[1].

Bu çalışmada iç ağ içerisindeki kullanıcıların ağda oluşturdukları trafik verisi dikkate alınarak bir nüfuz tespit işlemi gerçekleştirilmektedir. Çalışmada, Liao'nun yöntemine[5] benzer bir yöntem kullanılmıştır. Liao sistem çağrıları kullanırken bu çalışmada port kullanım istatistikleri kullanılmıştır. Ağdan toplanan verilerden veri özetleme teknikleri yardımıyla istatistik bilgiler elde edilmiştir. Modelin eğitim aşamasında birbirine benzeyen kullanıcılar aynı kümede birleştirilmiştir. Test aşamasında ise kullanıcının kendi kümesinden çıkıp çıkmadığı kontrol edilmiş ve kendi kümesinden çıkan kullanıcılar anormal olarak tespit edilmiştir. Yapılan deneysel çalışmada, ağdaki her bir kullanıcı kontrol altına alınıp bilinmeyen saldırılarla birlikte ağın yanlış kullanımları da tespit edilmiştir. Yapılan testlerde başarı oranları %96'larda çıkmaktadır.

Rahim KARABAĞ, Gebze Yüksek Teknoloji Enstitüsü Bilgisayar Mühendisliği Gebze Yüksek Teknoloji Enstitüsü İstanbul Caddesi, P.K. 141, Gebze, 41400 – Kocaeli, TURKEY, Ttel: +90 262 605 22 33 Fax: +90 262 653 84 90 E-mail: rkarabag@bilmuh.gyte.edu.tr

Hidayet TAKÇI, Gebze Yüksek Teknoloji Enstitüsü Bilgisayar Mühendisliği Gebze Yüksek Teknoloji Enstitüsü İstanbul Caddesi, P.K. 141, Gebze, 41400 – Kocaeli, TURKEY, Ttel: +90 262 605 22 33 Fax: +90 262 653 84 90 E-mail: htakci@bilmuh.gyte.edu.tr

Ibrahim SOĞUKPINAR, Gebze Yüksek Teknoloji Enstitüsü Bilgisayar Mühendisliği Gebze Yüksek Teknoloji Enstitüsü İstanbul Caddesi, P.K. 141, Gebze, 41400 – Kocaeli, TURKEY, Ttel: +90 262 605 22 33 Fax: +90 262 653 84 90 E-mail: ispinar@bilmuh.gyte.edu.tr

II. İLGİLİ ÇALIŞMALAR

Gerek ticari gerekse akademik ortamda geliştirilen birçok nüfuz tespit sistemleri mevcuttur. Kullandığı yöntemler ve uygulamaları farklı olsa da hepsinde amaç nüfuzu sisteme zarar vermeden tespit etmektir. Nüfuz tespit sistemleri temel olarak iki kategoride incelenmektedir. 1. kötüye kullanım tespiti 2. anormallik tespiti.[2,4]

- *Kötüye Kullanım Tespiti:* Nüfuzları tanımak için daha önceden bilinen saldırı imzalarından faydalanılır. İmza veritabanları güncel tutulması gerekmektedir. İlk kez oluşan saldırıları tespit etmek mümkün değildir[2,3].
- *Anormallik Tespiti:* Burada normal davranıştan farklılık gösteren davranışların saldırı olarak işaretlenmesi söz konusudur. Normal bir sistemde kullanıcı istekleri tahmin edilebilir istatistiksel değerlerle uyuşur. Normal davranıştan elde edilen kullanıcı örüntüleri temel alınarak veri trafiği gözlemlenir bir anormallik varsa tespit gerçekleşir. Bu yöntemin avantajı daha önceden tanınmayan saldırıların keşfedilmesi olasılığıdır. Dezavantajı ise yanlış alarmların sayısının yüksek olmasıdır[2,3].

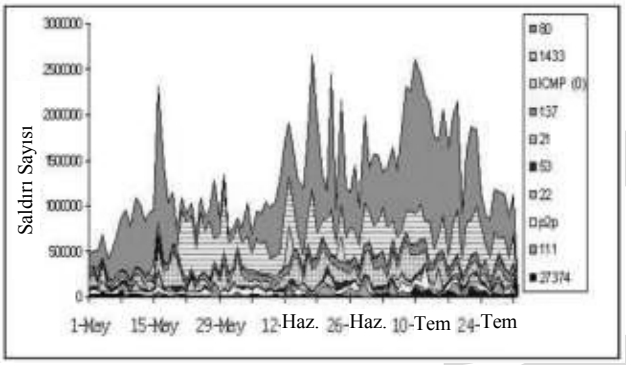
Nüfuz tespiti konusu ilgili olarak benzer çalışmalardan bazılarına kısaca bakmak gerekirse;

NSM(Network Security Monitor); ağı dinleyerek, ağın kullanımıyla ilgili bir örüntü geliştirir ve geçerli kullanımı onunla karşılaştırır. Elde edilen veri beklenen bağlantı verisiyle karşılaştırılır ve beklenen aralıkta çıkmayan her veri anormal olarak işaretlenir[1].

Liao 2002 yılında yaptığı çalışmasında sistem çağrılarına dayalı olarak nüfuz tespiti yaparken metin kategorilendirme tekniklerini kullanmıştır. Sistem çağrılarından hangilerinin

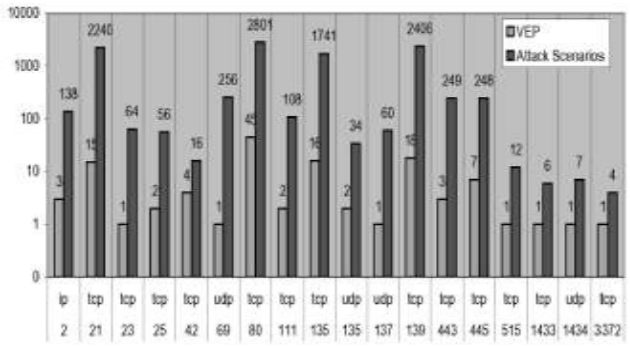
normal hangilerinin anormal olduğu kNN yöntemi ile bulunmuştur[5,6].

Kullanıcıları kümelemek için onları bazı öznitelikleri cinsinden vektörler yardımıyla sunmak lazımdır. Bu çalışmada öznitelik bilgisi olarak kullanılan port bilgileri ele alınmıştır. Öznitelik vektöründe hangi portların yer alacağına karar verebilme için Yegneswaran'ın çalışmasından faydalanılmıştır. Yegneswaran 2003 yılında Internet üzerindeki 1600 ağdan toplanan verilerin analizini yapmıştır. Bu analiz sonrasında her gün 25000 civarında saldırı gerçekleştiği saptanmıştır. Çalışmanın sonucuna göre en sık kullanılan port numaraları Şekil 1'de gösterildiği gibi bulunmuştur[8].



Şekil 1: Mayıs-Temmuz 2002 arasında 10 porta yapılan saldırı yoğunluğu[8].

2006 yılında Frederik Massicotte'nin yaptığı çalışmada Nüfuz tespit sistemlerinin değerlendirilmesinde portların önemi bir kez daha ortaya çıkmıştır. Bu açıklık sömürücü programlar ve saldırı senaryolarının gerçekleştiği port bilgileri Şekil 2'de görülmektedir[12].



Şekil 2: VEP ve atak senaryolarının veri kümesindeki port dağılımları[12].

2004 yılında Chen-g Lin yaptığı çalışmasında saldırı davranışlarından kural oluşturup bu davranışlara uygunluğun olup olmadığı tahmin sistemi ile kontrol edilir[11].

Jeffrey'nin 2004 de yaptığı çalışmada kullanıcı davranışları analizi yapılmış ve saldırgan kümeleri oluşturulmuş ve çözüm önerileri sunulmuştur[7].

III. ÖNERİLEN YÖNTEM

Nüfuz tespitinde daha önceki yöntemlerden farklı olarak bu çalışmada önerilen modelde ağdaki her bir kullanıcının ürettiği network trafiğinin analizi yapılmaktadır. Yöntemimiz temelde 4 aşamadan oluşmaktadır. İlk aşama ağ verilerinin toplanmasıdır. İkinci aşama kümelerin oluşturulmasıdır ve kullanıcıların bu küme bilgileri ile etiketlenmesidir. Bu işlem için önce kullanıcılar oluşturdukları trafik bilgilerine göre kullanıcı vektörleri ile sunulmuş ve ardından birbirine benzer kullanıcılar aynı kümelerde yer almak üzere kümeleme yapılmıştır. Kümeleme yöntemi olarak k-Means algoritması kullanılmış ve kullanıcılar üç kümeye ayrılmıştır. Üçüncü aşamada ise kullanıcı test verileri kNN yöntemi ile sınıflandırılarak test verilerinin yeni sınıfları bulunmuştur. Son aşamada eski sınıf bilgisi ile yeni bulunan sınıf bilgileri karşılaştırılarak eğer bu iki bilgi aynı ise kullanıcı normaldir, aksi takdirde anormaldir diyoruz.

Ağdan toplanan veri kullanıcı bilgilerini içermektedir. Kullanıcı vektörleri oluşturulurken her bir kullanıcının ağ trafiğinde ki kullanım istatistiklerinden faydalanılır. Kullanıcılar özniteliklerin tutulduğu bir vektör ile tanımlanır. $X(OZ_1, OZ_2, OZ_3,\ldots,OZ_M)$

Kullanıcı özellikleri: Her bir kullanıcı IP adresi ile tanımlanmaktadır. Kullanıcı özellikleri, kullanıcının ağ trafiği içerisinde oluşturduğu sinyallerden çıkarılır. Özellik çıkarımı için zaman serileri kullanılmıştır. Özellik çıkarımı şimdiden geriye dönük olarak çıkarılır ve çalışma saatleri esas alınarak son 1 günlük bağlantıların istatistikleri kullanılır. Kullanıcı tarafından oluşturulan paketlerin portlara göre bağlantı sayıları bulunur. TCP, SMTP, SSH, FTP, HTTP portu, gibi portlara yapılan bağlantı sayıları ile kullanıcı tanımlanır.

Özellik hesaplamasında Z, zamanda geriye dönük olarak alınan frekans sayısı, f_{ij} saniyedeki j sistemi için i özelliğinin frekansıdır. Aşağıda gösterilen formülde, Z adet frekans ortalaması j sisteminin i. özelliğini verir.

$$OZ_{ij} = \frac{\sum_{k=1}^{Z} {}^{k} f_{ij}}{Z} \quad (1)$$

Benzerlik: Sınıfı bilinmeyen X kullanıcısı k yakın komşu algoritmasına tabi tutulur. Bu kullanıcı için elde edilen eğitim verisinden onun profili oluşturulur. X kullanıcısının k adet en yakın komşusuna bakılır ve bu komşuların çoğunluğunun olduğu sınıfa X atanır. Her komşu için benzerlik ölçümü yapılır. Benzerlik ölçümü bilgi alma etki alanında sıklıkla kullanılan cosinus benzerlik bulma yöntemi ile hesaplanır.

D_j eğitim verileri için kullanıcılar *k-means* algoritmasından geçirilerek ait oldukları kümeler bulunur. Kümeleme algoritması çalıştırıldığında sistem yöneticisinin tanımladığı tüm kullanıcılar kendilerine en yakın komşularıyla bir araya getirilerek kümeleri oluşturulur ve bu küme değerleri sistem tablolarına eklenir. Artık sistemde kullanıcı ile birlikte bulunduğu kümesi de tutulur. Yöntem her an güncel verilerle analiz işlemini yaparak küme değerlerinin yenilenmesini sağlar. Böylelikle analizde en güncel veri kullanılmış olacaktır.

$$Sim(X, D_j) = \frac{\sum_{t_i \in (X \cap D_j)} x_i \times d_{ij}}{\|X\|_2 \times \|D_j\|_2} \quad (2)$$

t_i : X ve D deki i. ortak özelliği
x_i : X sistemindeki t_i özelliğinin ağırlığı
d_{ij} : D eğitim verisindeki sitemin t_i özelliğinin ağırlığı
$\|X\|_2$: X in Normu $\|X\|_2 = \sqrt{x_1^2 + x_2^2 + x_3^2 + \ldots}$
$\|D\|_2$: D nin Normu $\|D\|_2 = \sqrt{d_1^2 + d_2^2 + d_3^2 + \ldots}$

TABLO 1
AĞ KULLANIMININ KNN SINIFLANDIRMASIYLA NÜFUZ TESPİTİNDE KULLANILAN TERİMLERİN KARŞILIKLARI:

Terim	Ağ kullanımının kNN sınıflandırmasıyla nüfuz tespiti
X	Test kullanıcısı
D_j	Karşılaştırma yapılan sınıf j.
M	Seçilen özellik sayısı
f_{ij}	j kullanıcısı için i özelliğinin frekansı
Z	Zamanda geriye dönük olarak alınan frekans sayısı
OZ_{ij}	j kullanıcısı i. Özellik frekans ortalaması

K-Yakın Komşu (kNN) ile Sınıflandırma: Elimizde **X** kullanıcı vektörleri **D_j** sınıfları ile doğru olarak ilişkilendirilmiş örnekler bulunmaktadır. Aynı **j** sınıfı ile ilişkili olan **X** örüntülerinin birbirlerine benzer olduklarını söyleyebiliriz. Aynı sınıf örüntüleri genellikle bir bölgede kümeleşirler. Bu durum, sınıflandırılmamış **X** örüntülerini **en yakın k komşusu** olan **Dj** sınıfına ekleneceğini gösterir. D_j (OZ_1, OZ_2, OZ_3,….,OZ_M)

Anormallik Tespiti: Burada anormalliğin tespiti için bir kullanıcının eğitim sırasında bulunan kümesinden çıkıp çıkmadığı test edilmektedir. Küme dışına çıkma anormallik olarak kabul edilmektedir. X kullanıcısının test verileri ait olduğu sınıfa değil de başka bir sınıfa daha fazla benzerlik gösterirse anormal olarak işaretlenir ve sistem yöneticisine bildirilir. Bu tip anormal davranışlar gözlendiği anda uyarı sistemi devreye girerek sistem yöneticisine bildirilir. Anormallik tespiti için kullanılan algoritma aşağıda verilmiştir. Burada gelen X paketi bulunduğu D kümesi ile karşılaştırılır.

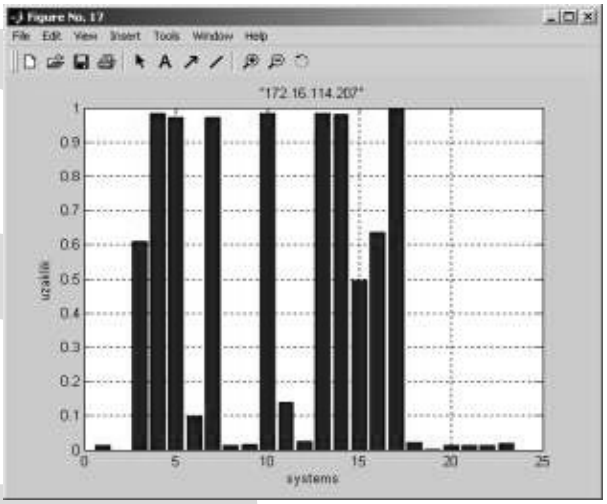
Eğitim verisinden D kümeleri belirlenir,
Her X kullanıcısının test verisini al,
Eğer X bilinmeyen bir kullanıcı ise
X anaormal dir;
Değilse
kNN yöntemi ile X kullanıcısının yeni sınıfını bul
Küme verilerini karşılaştır
Eğer Eşitse X normaldir,
Değilse X anormaldir,

IV. UYGULAMA VE DENEYSEL SONUÇLAR

Deneylerde DARPA (IDEVAL) 1999 verileri kullanılmıştır. Veri setleri toplam 5 haftalık bir süreyi kapsamaktadır, verilerin ilk 3 haftası eğitim (training) verileri, son 2 haftası da test verilerini içerir. Test verilerinde 58 değişik saldırı tipinde 200 adet saldırı mevcuttur. Bu saldırılar internetten ve saldırgan gruplarından aralıklarla toplanmış saldırı verileridir [9].

DARPA 99 verilerine öncelikle veri ön işleme adımları uygulanmıştır. Bu amaçla Ethereal programı kullanılmış ve veriler filtre işleminden geçirilmiştir. Böylelikle ilgili olmayan iç ağ dışındaki paketler ayıklanmıştır. Veriler daha sonra Matlab 6.5 ile analize tabi tutulmuştur.

Kullanım verilerinden her bir kullanıcıya ait özellikler çıkarılır. Bu veriler üzerinden nüfuz tespiti haricinde kullanıcılar hakkında istatistiksel değerler de elde edilebilir. Ağ kullanım bilgilerinin tutulduğu bu verilerden her bir kullanıcı için bir kullanıcı vektörü bulunur ve ardından kullanıcı vektörleri bir kümeleme algoritmasından geçirilerek (3 adet) kümeler bulunur. Kümeleme aşamasında kullanılan örnek benzerlik bilgilerinden biri Şekil 3. de gösteriştir.



Şekil 3: 172.16.114.207 IP adresli Kullanıcı Uzaklık grafiği

Buna benzer uzaklık ölçümleri kullanıldıktan sonra kümeleme işlemine geçilmiştir. Sistem yöneticisi eğitim verilerinden elde edilen bilgilere göre kümeleri tanımlar. Daha sonra test verileri kNN sınıflandırma algoritmasından geçirilerek kullanıcıların ait olduğu kümeler bulunur.

Kullanıcı test verileri sınıflandırılırken eğitim verileri ile test verilerinin kNN sınıflandırma sonuçları karşılaştırılır. Burada k için 1 den 10'a kadar değerler alınmıştır.

Tablo 2'den de görüldüğü gibi k sayısı değiştikçe küme grupları değişmektedir. K sayısı küçük alındığında bazı kullanıcıların farklı bir kümeye ayrıldığı görülmüştür. Ağı tanımlayacak çok yüksek olmayan çok da düşük olmayan bir değer uygun sonuç vermektedir.

TABLO 2
K DEĞERLERİNE GÖRE KULLANICI KÜMELERİ TEST SONUÇLARI

Sis.	Kume	K değerleri									
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
1	**1**	1	1	1	1	1	1	3	3	3	3
2	**2**	2	2	2	2	2	2	2	2	2	2
3	**3**	3	3	3	3	3	3	3	3	3	3
4	**3**	3	3	3	3	3	3	3	3	3	3

5	**3**	1	1	1	1	1	1	1	1	1	1
6	**2**	2	2	3	3	3	3	3	3	3	3
7	**3**	3	3	3	3	3	3	3	3	3	3
8	**1**	1	1	1	1	1	1	3	3	3	3
9	**2**	1	1	1	1	1	1	1	1	1	1
10	**3**	1	1	1	1	1	1	1	1	1	1
11	**3**	1	1	1	1	1	1	1	1	1	1
12	**2**	1	1	1	1	1	1	1	1	1	1
13	**3**	1	1	1	1	1	1	1	1	1	1
14	**3**	3	3	3	3	3	3	3	3	3	3
15	**3**	3	3	3	3	3	3	3	3	3	3
16	**3**	3	3	3	3	3	3	3	3	3	3
17	**3**	3	3	3	3	3	3	3	3	3	3
18	**2**	1	1	1	1	1	1	1	1	1	1
19	**1**	3	1	1	1	1	3	3	3	3	3
20	**1**	1	1	1	3	3	3	3	3	3	3
21	**1**	1	1	1	3	3	3	3	3	3	3
22	**1**	1	1	1	1	1	1	3	3	3	3
23	**1**	1	1	1	3	3	3	3	3	3	3
24	**X**										
25	**X**										
26	**X**										
27	**X**										

Alarm olarak verilen değerler tabloda gri renkle gösterilmiştir. X eğitim verisi bulunmayan kullanıcıları göstermektedir. Küme kolonunda koyu ve açık renkli olarak işaretlenen hücreler, saldırganlar ve saldırı yapılan kullanıcıları göstermektedir.

TABLO 3
TP,TN,FP,FN DEĞERLERI

	K değerleri						
	1	**2**	**3**	**4**	**5**	**6**	**7-8-9-10**
TP	12/13 0.92	11/13 0,85	11/13 0,85	11/13 0,85	11/13 0,85	12/13 0.92	12/13 0.92
TN	14/14 1	14/14 1	13/14 0,93	10/14 0,71	10/14 0,71	10/14 0,71	7/14 0,5
FP	0/14 0	0/14 0	1/14 0,07	4/14 0.28	4/14 0.28	4/14 0.28	7/14 0.5
FN	1/13 0,07	2/13 0,15	2/13 0,15	2/13 0,15	2/13 0,15	1/13 0,07	1/13 0,07

Burada doğru tespit edilen anormaller TP olarak gösterilir, doğru tespit edilen normaller TN, yanlış tespit edilen anormaller FP, yanlış tespit edilen normaller FN olarak alındığında tablo 3 elde edilir.

K değerleri değişmesi ile elde edilen doğruluk ve hata oranları tablo 4 de gösterilmiştir. Bu değerler ağda ki kullanıcı sayısına göre değişik ölçülerde alınabilir. Örnek uygulamada iç ağda 23 kullanıcı eğitim verisine dahil edilmiştir. Burada k'nın 7 den sonraki hesaplamaları hata ve doğruluk değerleri daha da kötüye gittiği görülmüştür. Optimum sonuç k'nın 1,2 ve 3 değerleri ile elde edilmektedir.

TABLO 4
DOĞRULUK VE HATA ORANLARI TPR VE FPR DEĞERLERİ

	K değerleri						
	1	**2**	**3**	**4**	**5**	**6**	**7-8-9-10**
Doğruluk	0,96	0,92	0,88	0,77	0,77	0,81	0,70
Hata	0,03	0,07	0,11	0,22	0,22	0,18	0,29
TPR	0,92	0,85	0,85	0,85	0,85	0,92	0,92
FPR	0	0	0,07	0,28	0,28	0,28	0,5

Deneysel çalışma sonuçlarına göre, örnek ağ verileri dikkate alındığında başarının kullanıcı sayısına ve seçilen k değerine bağlı olduğu görülmektedir. Darpa iç ağ verilerinden elde edilen sonuçlara göre k'nın 1,2 ve 3 değerlerinde FPR oranı % 0 ile % 0.07 arasında çıkmaktadır.

Bu çalışmada Liao kNN algoritması ile benzer algoritma kullanılmaktadır. Liao da sistem çağrıları gözlenerek anormallikler ile nüfuz tespiti yapılırken uygulamamızda farklı olarak ağdaki kullanıcıların oluşturduğu ağ kullanım veri kümeleri ile anormallik tespiti yapılmıştır. Liao tespit oranı %91.7 iken bu çalışmada tespit oranı %88-96 arasındadır.

V. SONUÇ VE ÖNERİLER

Yapılan uygulamada, bilinen Nüfuz tespit sistemlerine veri madenciliği tekniklerinin uygulanması, bilinmeyen saldırılar ve ağın yanlış kullanımları tespit edilmektedir. Uygulamada kümeleme yapılarak işlem yükü azaltılmış ve kullanıcıları tanımlamada esneklikler sağlamıştır. Çalışmada nüfuz tespiti yapılırken bir yandan da kullanıcıları ağ kullanım örüntüleri üzerinde istatistiksel bilgileri de elde edilmiş olur. Yöntem, tamamen denetimli çalışacağından ağda bulunan yetkisiz kullanıcılar engellenmiş olacaktır. Anormallik tabanlı sistemde daha önceden bilinmeyen saldırı türleri tespit edilebileceği gibi kullanıcıların ağ kaynaklarını yanlış veya ağa zarar verecek şekilde kullanması da engellenir. Virüs, trojan ve ağda oluşturulacak saldırı niteliği taşıyan diğer programları da ağ verisini analiz ederken engelleyecektir.

Yöntemin analizi ve kararlılığı, kullanıcı özellik tanımlamaları değiştirilerek arttırılabilir. Yapılan çalışmada elde edilen veriler kullanılarak ileriye dönük saldırı tahmin kuralları eklenebilir. Böylelikle ağda sadece anormallikler değil bunların yanında bazı kurallarda denetlenebilir. Aynı zamanda iç ağda çalışan bu yöntemi ağdaki farklı noktalara yerleştirerek dağıtık yapıya geçip ağ üzerindeki etkinliği arttırılabilir. Dağıtık oluşturulacak mimaride daha etkin saldırı önlemleri gerçeklenebilir.

KAYNAKLAR

[1] Axelsson S., "Intrusion Detection Systems: A Survey and Taxonomy", Technical Report Dept. of Computer Eng., Chalmers University, March, 2000.

[2] H.Takci, İ.Soğukpınar, "Saldırı Tespitinde Yeni Bir Yaklaşım",19.TBD Bilişim Kurultayı, 3-6 Eylül 2002 ,İstanbul

[3] M. Coşkun, İ. Soğukpınar, "Dağıtık Saldırı Tespit Sistemleri için bir Model", 19. Bilişim Kurultayı, İstanbul-Turkey, 2002.

[4] Kemmerer R.A., G. Vigna, "Intrusion Detection: A Brief History and Overview", IEEE Computer Special Issue on Security and Privacy, 2002.

[5] Y. Liao , V.R. Vemuri, "Use of K-Nearest Neighbor Classifier for Intrusion Detection", Computer and Security vol:21 no:5 PP:439-448,2002

[6] Y. Liao and V. R. Vemuri. Using text categorization techniques for intrusion detection. In Proc. 11th USENIX Security Symposium, August 2002

[7] Jeffrey M. Stanton, Kathryn R. Stam, Paul Mastrangelo and Jeffrey Jolton, "Analysis of end user security behaviours", Computers & Security, In Press, Corrected Proof, Available online 11 Sep.2004,

[8] Yegneswaran V., P. Barford, J. Ullrich, "Internet Intrusions: Global Characteristics and Prevelance", ACM SIGMETRICS, 2003

[9] DARPA Intrusion Detection Evaluation, web sitesi, 2006 "http://www.ll.mit.edu/IST/ideval/index.html" ,

[10] Beghdad Rachid, "Modelling and solving the intrusion detection problem in computer networks", Computers & Security, In Press, Corrected Proof, Available online 15 Sep.2004,

[11] Xiu-Zhen C., Qing-Hua Z, Xiao-Hong G, Chen-Guang Lin, "Forecast of intrusion behavior based on interactive knowledge discovery" Machine Learning and Cybernetics, Proceedings of 2004 International Conference on Volume 5, Issue , 26-29 Aug. 2004

[12] Frederic M, Francois G, Yvan L, Lionel B, Mathieu C, "Automatic Evaluation of Intrusion Detection Systems" Computer Security Applications Conference, 2006. ACSAC '06. 22nd Annual Dec. 2006