Kullanıcı Davranış Analizi ile Nüfuz Tespiti

Rahim Karabağ[1] İbrahim Soğukpınar[2]

[1,2]Bilgisayar Mühendisliği Bölümü,
Gebze Yüksek Teknoloji Enstitüsü,
No:101 41400 Çayırova Gebze/KOCAELİ

[1]rkarabag@bilmuh.gyte.edu.tr [2]ispinar@bilmuh.gyte.edu.tr

Anahtar sözcükler:Bilgisayar Güvenliği, Nüfuz Tespit sistemler, Anormallik Tespiti, Veri Madenciliği, kNN Kümeleme , Kullanıcı Davranış analizi,

Özet

Attacks on computer systems are increasing as the result of tools used for performing these attacks developing rapidly and becoming widespread. So the concept of information security became important in all sectors. All of the tools including firewalls, anti-virus software, intrusion detection systems, vulnerability scanners and encryption tools are aimed at providing the security of information.

In this work, an anomaly-based intrusion detection system is designed by using user behavior analysis. In the proposed method, statistical information about the users on the network is gathered from data collected from the network by using data mining techniques. User behaviors are constituted from this statistical information. kNN classification is used for clustering the user behaviors. Intrusion detection is performed by using anomaly based analysis on these clusters. If an intruder is detected, an alarm is created and system administrator is informed about this intrusion. As a result, by using the proposed method users on the network can be controlled. So the system can be prevented from intrusions and unwanted network usage errors.

1.Giriş

Saldırı, yetkisiz erişimlerle sistemin kırılmaya veya kaynakların yanlış kullanılmaya çalışılmasıdır. Saldırılar genellikle; hatalı ve eksik yetkilendirmelerde, zayıf şifreler kullanıldığında, sistem yanlış yapılandırıldığında ve yazılım kaynaklı açıklıklar bulunduğunda meydana gelir. Başarılı saldırı girişimleri nüfuz olarak tanımlanır. Saldırıların önlenmesinde kullanılan nüfuz tespit sistemleri güvenlik duvarının arkasında, ağ içerisinde çalışırlar [1,2].

Nüfuz Tespit sistemleri temel olarak iki kategoride incelenmektedir. 1. kötüye kullanım tespiti 2. anormallik tespiti.

- *Kötüye Kullanım Tespiti (Misuse Detection):* Nüfuzları tanımak için daha önceden bilinen örüntülerden faydalanılır. Kötüye kullanım tespitinde saldırı imzalarının tutulduğu saldırı veritabanları bulunur ve sistem verileri bilinen imzalarla karşılaştırarak saldırıları tespit eder. Belirli zaman aralıklarında imza veritabanları güncellenmesi gerekmektedir. İlk kez meydana gelen saldırıları tespit etmek mümkün değildir.[3,4]
- *Anormallik* (anomaly) *Tespiti:* Anormallik (anomaly) normal davranıştan sapma anlamına gelir. Burada normal davranıştan farklılık gösteren davranışların saldırı olarak işaretlenmesi söz konusudur. Normal bir sistemde kullanıcı istekleri tahmin edilebilir istatistiksel değerlerle uyuşur. Burada normal davranışın bilinmesi ve modellenmesi esastır. Bu 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 (false alarm/ positive) sayısının yüksek olmasıdır[3,4].

Nüfuz tespiti için çeşitli yöntemler kullanılmakta olup bunlardan birisi de veri madenciliğidir. Veri madenciliği tabanlı nüfuz tespitinde daha çok sınıflandırma ve kümeleme gibi teknikler kullanılır. Jeffrey ve arkadaşlarının 2004 de yaptığı çalışmada ağ kullanıcı davranışları belirli sınıflarla tanımlanmış ve bu sınıflara göre nüfuz araştırması yapmıştır[6]. Liao ve Vemuri'nin yaptığı çalışmada ise sistem çağrıları ile kümeleme yaparak nüfuz tespiti yapmıştır[5]. Ancak her iki çalışmada da ağdan toplanan kullanıcı verileri, kümeleme yapılarak incelenmemiştir.

Bu çalışmada, kullanıcı davranış analizi yapılarak nüfuz tespiti gerçekleştirilmiştir. Kullanıcıların ağ üzerine yaydıkları veri paketleri veri tabanında toplanır. Benzeşen kullanıcılar aynı kümede birleştirilir. Buradaki varsayım benzer davranış gösterenlerin benzer trafik oluşturacağıdır. Kümeleme için kNN algoritması kullanılmıştır. Trafik analizleri kullanıcı tabanlı yapılmaktadır. Analiz aşamasında kullanıcı verisi kendi bulunduğu küme değerleri ile karşılaştırılarak anormallik tespiti yapılmıştır.

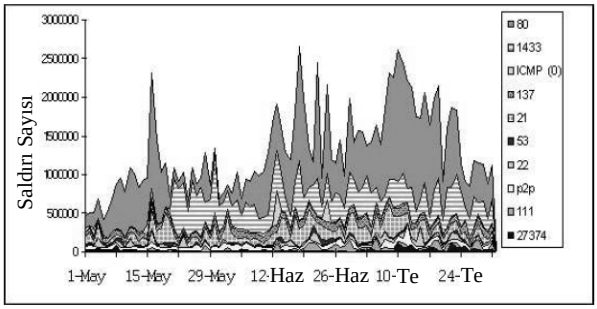
2. İlgili çalışmalar

Konu ile ilgi olarak literatürde değişik çalışmalar bulunmaktadır. İlgili olanların bazıları aşağıda açıklanmıştır.

NSM(Network Security Monitor)'de 1990-1994 arasına geliştirilmiştir. NSM 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[9].

Liao 2002 yılında yaptığı çalışmasında nüfuz tespiti için metin kategorize etme tekniklerini kullanmıştır. Sistem çağrıları içerisinde ki metin kNN ile kümelenmektedir. Daha sonra benzerlik ölçümleri yapılarak anormallik tespiti yapılmıştır[7].

2003 yılında Yegneswaran tarafından yapılan bir çalışmada internet üzerindeki 1600 ağdan toplanmış verilerin analizi yapılmıştır. İnternet üzerinde her gün 25000 civarında saldırı gerçekleştiği saptanmıştır [8]. Bu çalışmadan alınan aşağıdaki grafikte sadece yoklama (probe/scan) saldırısı göz önüne alındığında Mayıs-Temmuz ayları arasındaki port numaralarına karşı düşen saldırı yoğunluğu verilmiştir.

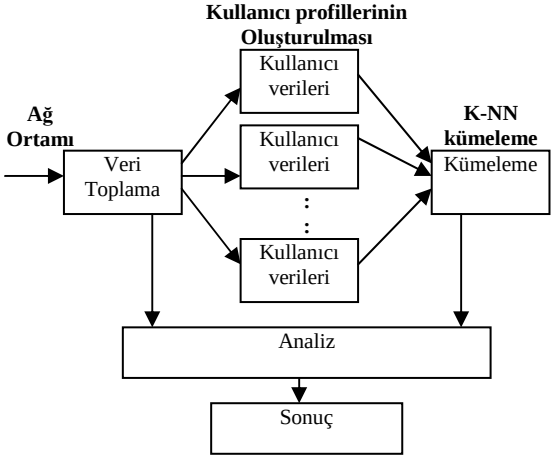


Şekil 1: Mayıs-Temmuz 2002 arasında 10 porta yapılan saldırı yoğunluğu [8].

Bizim yaptığımız çalışmada ise Liao'nun kullandığı kümeleme yöntemlerini ağdaki kullanıcı verileri üzerinde gerçeklenmesidir. Liao'daki sistem çağrıları yerine kullanıcıyı tanımlayıcı gelen port frekansları kullanılmıştır. Yegneswaran'in çalışmasında belirlenen saldırının gerçeklendiği portlar dikkate alınarak bu portların frekansları her kullanıcıya özel olarak tutulmuştur[8].

3. Önerilen Yöntem

Nüfuz tespitinde daha önceki yöntemlerden farklı olarak sistemimizde kullanıcı temelli ağ analizi yapılmaktadır. Ağ içerisinde kullanıcıların oluşturduğu veriler incelenerek her bir kullanıcının bir profili çıkarılır. Daha sonra bu kullanıcı profilleri kNN yöntemi ile kümeleme uygulanarak kullanıcı kümeleri elde edilir. Sitemin blok diyagramı Şekil 2'de gösterilmiştir. kNN kümelemeyi 2002 Liao ve Verumi tarafından yapılan nüfuz tespit sisteminde ağdan toplanan sistem çağrılarını kümelerken kullanmıştır. İki uygulamanın mukayesesi Tablo 1' de gösterilmiştir.



Şekil 2: Kullanıcı davranış analizi ile Nüfuz tespit sistemi modeli

Ağdan toplanan veri kullanıcı bilgilerini içermektedir. Kullanıcı profilleri oluşturulurken her bir kullanıcının network trafiğinde ki kullanım istatistiklerinden faydalanılır. Kullanıcı bilgilerinin tutulduğu bir dizi ile tanımlanır.

Kullanıcı: $X(OZ_1, OZ_2, OZ_3,\ldots,OZ_M)$ (1)

Tablo 1: kNN ile yapılan nüfuz tespit sistemleri:

Terim	Sistem çağrılarına kNN sınıflandırılmasıyla nüfuz tespiti	Kullanıcı Davranışlarına kNN sınıflandırmasıyla nüfuz tespiti
X	Test işlemi	Kullanıcı
$\mathbf{D_j}$	j . eğitilmiş işlem	Karşılaştırma kümesi j.
N	Toplam işlem Sayısı	Kullanıcı Sayısı
M	farklı sistem çağrılarının toplam sayısı	Kullanıcı için seçilen özellik sayısı
$\mathbf{n_i}$	i. sistem çağrısının geçtiği işlem sayısı	i özelliğinin geçtiği kullanıcı sayısı
f_{ij}	i. sistem çağrısının j işlemindeki frekansı	j kullanıcısı için i özelliğinin frekansı
T	Eşik Değer	küme farkı hesabı için kullanılan eşik
a_{ij}	J işlemindeki i. Sistem çağrısının ağırlığı	j kullanıcısı için i özelliğinin ağırlığı
Z		Zamanda geriye dönük olarak alınan frekans sayısı
$\mathbf{OZ_{ij}}$		j kullanıcısı i. özellik frekans ortalaması

Kullanıcı Davranışı : Kullanıcı MAC adresi ile tanımlanan IP adresi ile gösterilir. Kullanıcının davranışları, ağ trafiği içerisinde oluşturduğu trafik sinyallerinden çıkarılır. Özellik için zaman serileri kullanılır. Özellik çıkarımı şimdiden geriye dönük olarak çıkarılır ve çalışma saatleri esas alınarak son 1 günlük bağlantıların istatistikleri kullanılır. Gelen paketlerin porta göre bağlantı sayıları bulunur. TCP, SMTP port , SSH port, FTP port, HTTP port, gibi bağlantı sayıları kullanıcıyı tanımlar.

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

$$OZ_{ij} = \frac{\sum_{k=1}^{Z} {}^{k} f_{ij}}{Z} \qquad (2)$$

$$a_{ij} = OZ_{ij} x \log\left(\frac{N}{n_i}\right) \qquad (3)$$

Kullanıcı özelliklerinin tanımlayıcı olduğunu belirlerken her bir özelliğe bir ağırlık tanımlanır. Bu tanımlama da A matrisinde tutulur. Burada N Kullanıcı sayısı, n_i, i özelliğinin geçtiği kullanıcı sayısı, OZ_{ij} özellik frekans ortalamasıdır. A matrisinde her bir özelliğin kullanıcılardaki ağırlıkları olan a_{ij} değerleri tutulur.

Benzerlik : Kümesi belirlenemeyen X kullanıcısı k yakın komşu algoritmasına tabi tutulur. Bu kullanıcı için elde edilen eğitim dokümanından kullanıcının profili oluşturulur. K adet yakın komşusuna bakılır ve bu komşuların çoğunluğun olduğu kümeye dahil edilir. Her komşu için benzerlik ölçümü yapılır. Benzerlik ölçümü cos. değeri ile hesaplanır.

$$Sim(X, D_j) = \frac{\sum_{t_i \in (X \cap D_j)} x_i \times d_{ij}}{\|X\|_2 \times \|D_j\|_2} \qquad (4)$$

t_i : X ve D deki i. ortak özelliği
x_i : X kullanıcısındaki t_i özelliğinin ağırlığı
d_{ij} : D kullanıcısındaki 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 $\|D\|_2 = \sqrt{d_1^2 + d_2^2 + d_3^2 + \ldots}$

K-Yakın Komşu (kNN) ile Kümeleme: Elimizde **X** örüntüleri $\mathbf{D_j}$ 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 dahil edileceğine işaret eder. D_j (OZ_1, OZ_2, OZ_3,….,OZ_M)

D_j kümeleri için kullanıcı verileri aşağıda belirtilen kNN kümeleme algoritmasından geçirilir ve ait olduğu kümeler bulunur.

D={t₁, t₂, ... t_m} // Küme elemanları kullanıcılar
A // elemanlar arasındaki uzaklıkların tutulduğu matris
T // Eşik değer
SK // oluşan kümeler
X₁ := {a₁, a₂, ... a_m}; // kullanıcı
k = 5; // k adet yakın komşu bulunur

1 den n kullanıcı için hesapla //n kullanıcı sayısı
ai= sim(t_i,t_xi) // X. kullanıcı için *A i* kullanıcısının uzaklık matrisi

A uzaklık matrisinden en büyük k adet komşuyu bul
Benzelik averajını bul sim_avg=(X,D)

J adet Küme ile karşılaştır.
Eğer sim_avg > Eşik değer se // max benzerlik eşik değerden büyükse
$SK_j = SK_j \; U \; X_i$ // Xi kullanıcısı SK_j kümesine dahil edilir.
Sonuç:
SK = {X₁,X₂,X₃} //SK kümesi kullanıcı listesi

Kümeleme algoritması çalıştırıldığında sistem yöneticisinin tanımladığı tüm kullanıcılar kendilerine en yakın komşularıyla bir araya getirilerek kümeleri oluşturulur ve bu küme değerleri kullanıcı tablolarına eklenir. Artık sistemde kullanıcı ile birlikte bulunduğu kümesi de tutulur. Sistem her an güncel verilerle analiz işlemini yaparak küme değerlerinin yenilenmesini sağlar. Böylelikle analizde en güncel veri kullanılmış olacaktır.

Bu işlem sonrasında her bir kullanıcının kümeleri hesaplanır ve küme merkezi her seferinde tüm kullanıcıların ortalama değerleri ile bulunur.
D_j (Ort(OZ_1), Ort(OZ_2), ….,Ort(OZ_M))

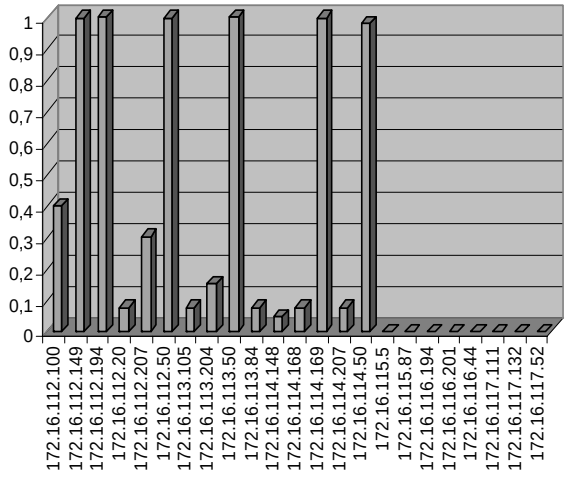
Anormallik Tespiti: Her bir kullanıcı verileri ait olduğu küme normal alınarak kontrol edilir. X Eğitim verisi içerisinde bulunmayan bir kullanıcı ise anormal olarak işaretlenir ve sistem yöneticisine bildirilir. Anormallik tespiti bir kullanıcının kendi kümesi arasındaki uzaklığın bir eşik değeri aşıp aşmamasına bakılarak tespit edilir. Eşik değer aşılırsa normal dışı uygulama olacaktır ve kullanıcının kendi kullanım yetkileri dışına çıktığı anlamına gelecektir. $Sim(X,D_j) <= T$ T: Eşik değer Eşik değer kullanıcı merkezine en uzak kullanıcı değerine bağlı olarak sistem yöneticisi tarafından verilir. 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 kullanıcısı test verisini al,
Eğer X bilinmeyen bir kullanıcıysa
X anaormal dir;
Değilse
X her kullanıcı ile D kümesi için eğitim verisini al
Benzelik(X,D_j) hesapla
Eğer Benzerlik >= Eşik değer se
X normaldir,
Değilse
X anormaldir,

4. Uygulama ve Deneysel Sonuçlar

Deney veri seti olarak DARPA'nın 1999 yılında NTS'ler için bir karşılaştırma ortamı sunan IDEVAL veri setleri kullanılmıştır. Ağda bulunan bilgisayarlar üzerinde SunOS, Solaris, Linux, ve Windows NT çalışmaktadır. Veri setleri toplam 5 haftalık bir süreyi kapsamaktadır, ilk 3 haftası eğitim (training) verileri, son 2 haftası da test verileridir. 1. hafta ve 3. hafta saldırı içermemektedir. 2. hafta bazı saldırılar içermekte ve bu saldırılar ayrıca bir dosyada işaretlenmiştir. Bu kısım değerlendirmeye alınacak sistemlerin kendi başarımlarını test etmeleri içindir. Geriye kalan 4. ve 5. haftalarda ise 58 değişik saldırı tipinde 200 adet saldırı mevcuttur. Bu saldırı yazılımları internet ortamından ve hacker sitelerinden toplanmış saldırılardır ve sisteme aralıklarla enjekte edilmiştir [10].



Şekil 3: 172.16.112.194 IP adresli Kullanıcı Uzaklık grafiği

Kullanılan veriler kullanıcı bazlı olarak veritabanında depolanır. Bu veriler üzerinden nüfuz tespiti haricinde veri madenciliği yöntemleri ile kullanıcı hakkında istatistiksel değerlerde elde edilebilir. Kullanıcı davranışlarının tutulduğu bu verilerden her bir kullanıcı için uzaklık ölçümleri hesaplanır. Şekil 3'de gösterilen kullanıcı uzaklık grafiğinde benzer kullanıcılar birbirine yakın çıkmaktadır.

Bu uzaklık ölçümleri kullanılarak kümeleme işlemine geçildi. Kullanıcı verileri kNN kümeleme algoritmasından geçirildi ve ait olduğu kümeler bulundu. Benzer kullanıcıların oluşturduğu kümeler belirlenmiştir.

Kümeleme işlemi gerçekleşirken k sayısı 3, 5, 10 olarak üç farklı şekilde test edilmiştir.

Tablo 2: K=3 için belirlenen kullanıcı kümeleri

Küme	Kullanıcılar
A	1, 11
B	2, 3, 9, 6, 13, 15
C	5, 8, 7, 10, 12, 14, 4
D	16
E	17, 18, 20, 21, 23, 22
F	19

Tablo 3: K=5 için belirlenen kullanıcı kümeleri

Küme	Kullanıcılar
A	1, 5, 8, 11, 7, 10, 12, 14, 4
B	2, 3, 9, 6, 13, 15
C	16
D	17, 18, 20, 21, 23, 22
E	19

Tablo 4: K=10 için belirlenen kullanıcı kümeleri

Küme	Kullanıcılar
A	1, 5, 8, 11, 7, 10, 12, 14, 4 , 2, 3, 9, 6, 13, 15
B	16
C	17, 18, 20, 21, 23, 22
D	19

Tablo 2,3 ve 4'den görüldüğü gibi k sayısı değiştikçe küme grupları değişmektedir. Bu kullanıcı yoğunluğuna ve birbirlerine olan benzerlik değerlerine göre en uygun değer belirlenir. K sayısı küçük alındığında bazı kullanıcıların farklı bir kümeye ayrıldığı görüldü. Kullanıcı karakteristiğini belirleyecek çok yüksek olmayan çok da düşük olmayan bir değer uygun sonuç vermektedir. Bizim uygulamamızda k=5 değerinde uygun çözüm bulunmuştur. K değeri her ağ trafiğinde farklı olabilir. Sistem yöneticisi kullanıcı yoğunluğuna göre uygun değeri belirler.

Kümeler oluşturulduklarında 16 ve 19 no'lu kullanıcıların hiçbir kullanıcı ile benzeşemediği görüldü bu kullanıcılar ayrı bir küme gibi değerlendirilmektedir. Diğer kullanıcılarda davranışlarına göre kendilerine uygun kümelere yerleştirilmiştir. K değerine bağlı olarak bazı kullanıcılar değişik kümelerde yer almıştır. Bu

kullanıcıların kümeleme işleminde yakın komşu değerlendirmesine göre değişmektedir.

Yapılan uygulamada anormallik tespiti için algoritma çalıştırıldığında aşağıdaki sonuç bulunmuştur. Burada görünen 4 kullanıcı tespit edilmiştir. İlk iki kullanıcı kendi küme özellikleri dışına çıkan kullanıcılar. Diğer ikisi sisteme izinsiz girmiş kullanıcılardır.

Tablo 5: K=5 anormallik analiz sonuçları

Kullanıcı(IP No)	Benzerlik	Onay
172.16.112.100	0,87	Normal
172.16.112.149	**0,05**	**Anormal**
172.16.112.194	0,996	Normal
172.16.112.20	**0,001**	**Anormal**
172.16.112.207	0,85	Normal
172.16.112.50	0,995	Normal
172.16.113.105	0,85	Normal
172.16.113.204	0,85	Normal
172.16.113.50	0,995	Normal
172.16.118.10	**X**	**Anormal**
172.16.113.80	**X**	**Anormal**

Sistem yöneticisi tarafından kullanıcı istatistikleri dağılımına bakılarak bir eşik değer tanımlanır. Küme ortalamaları ile kullanıcı değerleri arasındaki benzerliğin en az 0,87 olduğu görülmüştür. Kullanıcı davranış değişimleri de düşünülerek sistemimizde eşik değeri 0,8 alınmıştır. Yukarıdaki tabloda kullanıcı kontrolleri yapılarak anormallikler tespit edilen değerler gösterilmiştir. Sisteme daha önce girişi yapılmayan kullanıcılar için değerlendirme yapılmaz. Bu kullanıcı doğrudan anormal olarak tespit edilip sistem yöneticisine bildirilir.

5. SONUÇ

Bu çalışmada önerilen yöntem, bilinen Nüfuz tespit sistemlerine veri madenciliği tekniklerinin uygulanmasını ve gerçek zamanlı kullanıcı analizinin yapılmasını sağlamaktır. Yapılan çalışmada, bir yandan nüfuz işlemleri tespiti yapılırken bir yandan da kullanıcı örüntüleri üzerinde istatistiksel bilgileri de elde edilmiş olur. Sistem tamamen kullanıcı denetimli çalışacağından ağda bulunan yetkisiz kullanıcılar engellenmiş olacaktır. Anormallik tabanlı sistemimizde daha önceden bilinmeyen saldırı türleri tespit edilebileceği gibi kullanıcının da sistem kaynaklarını yanlış veya sisteme zarar verecek şekilde kullanması da engellendi. Virüs, trojan ve ağda oluşturulacak saldırı niteliği taşıyan diğer programları da ağ verisini analiz ederken engelleyecektir.

Sistemin analizi ve kararlılığı zamanla kullanıcı özellik tanımlamaları değiştirilerek arttırılabilir. Aynı zamanda iç ağda çalışan bu sistemi ağdaki farklı noktalara yerleştirerek dağıtık sisteme geçip ağ üzerindeki etkinliği arttırılabilir. Dağıtık oluşturulacak mimaride daha etkin saldırı önlemleri gerçeklenebilir.

KAYNAKLAR

[1] Stallings W., “Network Security Essentials”, Prentice Hall, 2003

[2] Mustafa Coşkun, İbrahim Soğukpınar, “Dağıtık Saldırı Tespit Sistemleri için bir Model”, 19. Bilişim Kurultayı, İstanbul-Turkey, 2002.

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

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

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

[6] 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,

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

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

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

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

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