Kuzey Kıbrıs Geniş Bant Kullanıcılarının Davranışları

Devrim Seral[1]

[1]Bilişim Sistemleri Mühendisliği Bölümü, Uluslararası Kıbrıs Üniversitesi, Kıbrıs

[1]e-posta: dseral@ciu.edu.tr

Özet

Geniş bant İnternet erişimi artık sıradan bir erişim yöntemi haline gelmiştir. Geniş bant erişimi olan kullanıcılar, sunulan her türlü servise hızlı ve sorunsuz şekilde ulaşmak istemektedirler. Bu erişim modelinde, kullanıcıların yarattığı trafik ve erişim davranışları, servis sağlayıcılar ve ağ sağlayıcılar için büyük önem taşımaktadır. Bu çalışmada, Kuzey Kıbrıs'ta geniş bant İnternet erişimi olan kullanıcıların, erişim davranışları iki açıdan ele alınmıştır. Birincisi, ağ üzerinden toplanan veri izleri yardımı ile İnternet erişiminin yoğunlaştığı servisleri göstermek diğeri ise yine bu ağ verilerini kullanarak güvenlik analizi yapmak olacaktır.

1. Giriş

Günümüzde İnternet hayatımızın her evresine girmiş ve vazgeçilmez unsurlarından biri olmuştur. İnternet günlük hayatımızı kolaylaştırmakta ve bize birçok servis sunmaktadır. Bu sunulan servislerin kullanım sıklıkları ve metodları her bireyde farklı şekilde olabilmektedir. Bunların bilinmesi; servisleri verenler, kullanıcılar ve ağ altyapısını sağlayanlar'a servis kalitesini, sürekliliğini ve performansını artırılması yönünde yardımcı olmasından dolayı büyük önem taşımaktadır.

Dünyada İnternet geniş bant erişimi yapan kullanıcı sayısının 2009 yılı sonunda beşyüz milyona ulaşması öngörülmektedir. [1]. Geniş bant İnternet kullanım seviyesi ile ülkelerin bilişim teknolojilerindeki sırası arasında doğru orantılı bir ilişki bulunmaktadır.

Kuzey Kıbrıs'ta geniş bant İnternet erişimi çok yeni bir olgudur ve erişim davranışları ile ilgili olarak şu ana kadar herhangi bir çalışma yapılmamıştır. Bu nedenle çalışmanın temel konusu Kuzey Kıbrıstaki geniş bant kullanıcıların İnternet erişim davranışları olacaktır.

Kuzey Kıbrısta geniş bant İnternet hizmeti şu anda üç şekilde verilmektedir:

- Bakır telefon kablosu üzerinden verilen ADSL ve GHDSL servisleri.
- 802.11 a/b/g kullanılarak verilen kablosuz servisler.
- 3G Mobil geniş bant servisleri

Kuzey Kıbrıs'ta ADSL hizmetinin verilmesine Nisan 2007'de başlanmıştır[1]. Temmuz 2009 itibari ile ADSL port sayısı 11878'dir[2].

[1] http://www.kktctelekom.com/hizmetler_adsl_s.htm

[2] http://www.kktculastirma.org/04_telekom/raporlar/index.html

Bu çalışmada geniş bant için en yaygın olarak kullanılan ADSL hizmetinin ağ verileri kullanılacaktır.

İnternet trafik akışlarının nasıl davranış gösterdiği halen üzerinde çalışmaların devam ettiği konulardan biridir. Bu çalışmalar "İnternet Trafik Tanımlama" olarak isimlendirilir [2]. Trafik tanımlamanın yapılmasındaki temel amaç kapasite ihtiyaçlarını belirleyebilmek ve altyapı sorunlarını tespit edebilmektir.

Ağ trafiğini doğrudan etkileyen diğer bir faktör ise ağ üzerinde oluşan düzensizliklerdir. Ağ sistemlerine erişim, altyapı sorunlarının dışında ağı kötüye kullanma yada ağ üzerinde düzensizlik yaratılarak kesintiye uğratılabilir. Bunların önüne geçmek için ağ trafiğini izlemek ve analiz etmek önem kazanmaktadır. Hızlı ve verimli çalışan analiz sistemlerinin varlığı, bu sorunların etkin bir şekilde ağa zarar vermesini engelleyebilmektedir. Bu şekilde çalışan sistemlere saldırı tespit sistemleri adı verilmektedir [3]. Ağ saldırı tespit sistemleri, imza tabanlı ve düzensizlik tabanlı olarak sınıflandırılabilirler [4]. İmza tabanlı sistemler, bilinen saldırı türlerine göre yazılan kurallar ile çalışırlar [5].

Bu makalede, ADSL hizmeti veren bir ISP'den alınan pasif ağ verileri üzerinde çalışma yapılmıştır. Ağ verileri tcpdump veri formatında tutulmuştur [6]. Makalenin ilk bölümünde trafik tanımlama yöntemleri ve saldırı tespit sitemleri konusunda kısaca bilgi verilmiştir. Sonraki bölümde ise analiz için kullanılan yöntem ve araçlar konusunda bilgi verilmiştir. Dördüncü bölümünde ise trafik verileri ile ilgili bulgular verilmiştir.

2. İnternet Trafik Tanımlama Yöntemleri ve Saldırı Tespit Sistemleri

Bu bölümde ilk önce İnternet trafik tanımlama yöntemlerine yer verildikten sonra saldırı tespit sistemleri ele alınacaktır.

2.1. İnternet Trafik Tanımlama Yöntemleri

Paket ağlarındaki trafik tanımlama ile ilgili ilk çalışmalardan biri de Jain ve Routhier'in MIT'de yaptığı çalışmadır [7]. Bu çalışmada yerel ağda yapılan ölçümler sonucu ağdaki trafiğin Poisson [8] ya da Birleşik Poisson dağılımı ile modellenemeyeceğini, bunun yerine "paket treni" modelini ortaya koymuşlardır [7,8].

Bu modelde ağ içindeki iki nokta arasındaki paket akışının olduğu kabul edilir. Bu paket akışlarının da veri taşıyan trenler ile yapıldığı varsayılır. Paketin gelişi ile sonraki paketin aynı trenin dönüşüne ait olma olasılığını vardır. Bu da ağ protokollerinin istek-cevap doğasından gelmektedir. Bu keşiften sonra ağ cihazlarında kaynak ve hedef adresi önbelleklemesi çok önem kazanmışdır.

Yine MIT'den Feldmeier'in yaptığı çalışmalarda [9] ağ yönlendiricisi üzerinde birkaç "hedef adres, çıkış portu" şeklinde satır içeren basit bir önbelleğin bile performansı ciddi biçimde artırdığı gözlemlenmiştir. Burada hedef adresin yeniden kullanım sıklığı analiz edildi ve LRU önbelleğin yönlendirme tablosuna erişimini azalttığı belirlenmiştir.

Mogul ağ yerelliğini işlem seviyesinde araştırmıştır. Referans yerelliğinin sistem adresi seviyesinde olduğunu ortaya koymuştur. Yerel ağdan topladığı veriler üzerinde yaptığı analizlerde %75 oranında paketin hedef port numaralarının aynı ve paketlerin geldiği sistemlerde de kaynak port numaralarının aynı olduğunu tespit etmiştir [10].

CAIDA'dan Broido, Hyun ve Claffy'nin [11] ip trafiği üzerinde yaptıkları çalışmalarda trafik akış yaratan kaynakların diğerlerine göre farklılığının Pareto kuralı [12] 80/20 ile benzerlik gösterdiğini (%80 trafik %20 kaynak) bulmuşlardır. Daha derin araştırmaları sonucu bu oranların bazı yerlerde 90/10 hatta 95/5 ulaştığını da tespit etmişlerdir [11].

2.2. Ağ Saldırı Tespit Sistemleri

Ağ trafiğinde oluşan düzensizliği inceleyerek, saldırı tespit etmek için değişik çalışmalar yapılmıştır. Bu çalışmaların birçoğunda istatistiksel yöntemler ve trafik örnekleme kullanılarak analiz yapılmaya çalışılmıştır [13,14]. Yönlendiricilerden toplanan akış verileri ve ip paket başlıkları bu araştırmaların temelini oluşturmaktadır.

İz eşleştirme, normal olmayan trafiğin tespit edilmesinde kullanılan bir yöntemdir. Bu yöntemde motivasyon ağda bilinen servis ve ip bloklarının akış verileri ile karşılaştırılmasına dayanır. Mevcut servislere ait port ve ip bilgileri oluşturulan bir veritabanı yardımıyla akış verileri ile karşılaştırılır. Veri tabanında bulunmayan port veya ip adreslerine gelen veya giden trafik şüpheli olarak değerlendirilebilir. Örneğin sadece 80 portundan hizmet veren bir sunucunun 3306 portuna bir istek gönderildiğinde uyarı sistemi devreye girip şüpheli durumu bildirebilir. Bu yöntem ağ tarama tespitinde kolayca kullanılabilir.

İz eşleştirmede bir diğer yaklaşım, TCP bayraklarından (flags) yararlanarak örnekleme veritabanı oluşturmaktır. TCP Protokolünde, Three-way-handshake [15] prosedürünü tamamlamayan, sürekli SYN paketleri gönderen istemciler veya sürekli SYN paketi alan sunucular normal olmayan trafiğin habercisidir. Akış verilerindeki TCP bayrakları ile karşılaştırma yapıldığında belirli bir eşik değerin üzerindeki paket türleri düzensiz olarak kabul edilebilir. Genellikle böyle bir durum DoS veya DDoS saldırısını işaret eder.

Port ve TCP bayrağı yaklaşımına benzer bir yaklaşım IP adresleri için de uygulanabilir. Kaynak adresi IANA tarafından rezerve edilmiş ip kümelerinden [16] gelen trafik düzensiz olarak değerlendirilebilir. Ayrıca ağa ait fakat kullanılmayan ip adreslerine doğru yapılan trafik ağ taraması veya solucan aktivitesini işaret edebilir. IP veritabanı örneklemesi dışarıdan gelen saldırılara karşı etkili olabildiği gibi aynı yaklaşımla iç ağdan yapılan saldırıların da tespitinde önemli rol oynayabilir.

Saldırı tespit sistemlerinde kullanılan bir diğer yöntemde paket yükünün (payload) önceden tespit edilmiş ve ona göre yazılan imzalar yardımı ile sorunlu olup olmadığının tespit edilmesidir [17]. Ancak çok fazla sistem kaynağı tüketmesinden dolayı, yüksek hızlı ağlarda bu yöntemle saldırı tespiti yapmak çok güçtür.

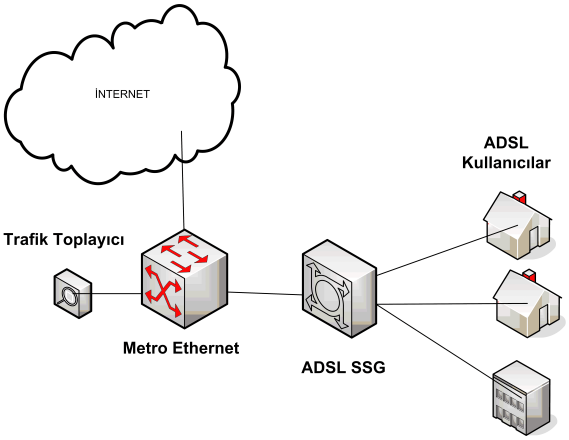
Bu çalışmada analiz, aktif ağ üzerinde değil pasif ağ verileri üzerinde yapıldığı için paket yükü verilerinden de yararlanılmıştır.

3. Yöntem ve Araçlar

Bu kısımda trafik toplama yöntemi ve analizde kullanılan araçlardan bahsedilecektir.

3.1. Trafik Toplama Yöntemi

Trafik verileri üzerinde analiz yapılabilmesi için öncelikle kullanıcıların yarattığı trafiğin toplanması gerekmektedir. Şekil 1'de trafik toplama sisteminin yapısı verilmiştir. Trafik verileri bir metro ethernet ağ anahtarı üzerindeki aynalama (mirror) ucuna bağlanan bir bilgisayar aracılığıyla alınmıştır.



Şekil 1: **Trafik toplama sistemi.**

Trafik toplayıcı cihaz üzerine İnternet trafik verilerini toplayıp sonradan analiz edebilmek için açık kaynak kodlu Snort yazılımı kullanılmıştır [18].

İnternet sağlayıcının metro ethernet çıkış hızı 50 Mbps ve trafik toplanırken erişim yapan ortalama uç sayısı 700'dü. Trafik toplama işlemi 7 saat sürmüştür. Bu süreden sonra trafik toplayıcı makinenin sabit diskinin dolmasından dolayı, trafik toplama işlemine devam edilememiştir.

3.2. Trafik Analizinde Kullanılan Araçlar

İnternet trafik verilerini kullanarak kullanıcıların hangi servisleri daha fazla kullandığını görebilmek için geliştirilmiş Ntop yazılımı kullanılmıştır [19]. Ntop yazılımı ile pasif tcpdump verileri işlenerek anlamlı hale getirilmiştir.

Yine bu pasif tcpdump verileri Snort yazılımı tarafından işlenerek trafik toplama süresince oluşan anormalik ve saldırılar veritabanına kaydedilmiştir. Veritabanına kaydedilen veriler Base uygulamasi ile anlamlandırılmıştır [20].

4. Analiz Bulguları

Geniş bant kullanıcılarınn trafik davranışları iki şekilde incelenmiştir. Birincisi kullanımın yoğunlaştığı servisler, ikincisi ise dışardan gelen yada bu servisleri yapan kullanıcıların yaptıkları saldırılar olarak verilmiştir.

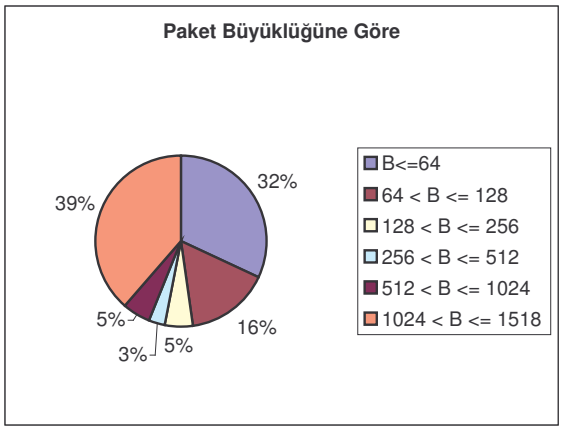
4.1. Geniş Bant Kullanıcılarının Servis Kullanım Davranışları

Servis kullanım davranışları incelenirken Ntop yazılımından yararlanılmıştır. Ntop yazılımı ile yaklaşık 200 milyon paket işlenerek aşağıda verilen sonuçlar elde edilmiştir.

*Tablo 1:***Paket Türüne Göre**

Paket Türü	Paket Sayısı	Yüzdesi (%)
Unicast	199,043,871	99.9994
Multicast	1	0.0
Broadcast	3,279	0.0016

Tablo 1 paket türüne göre paket sayılarını göstermektedir. ADSL kullanıcılarının yarattığı trafiğin tamamen Unicast olduğu ve Broadcast yada Multicast trafiğin bütüne göre hiç sayılabilecek kadar az olduğu tespit edilmiştir.



Şekil 2: **Paket büyüklüklerine göre dağılım grafiği.**

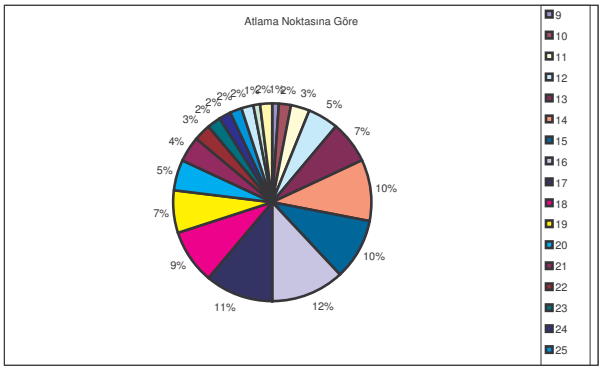
Şekil 2'de paket büyüklüklerine göre trafik incelendiğinde paket boyutlarının 64 Byte'dan küçük ve 1024 Byte'dan büyük kısımlarda yoğunlaştığı görülmektedir. 64 Byte'dan küçük verilerin DNS sorgusu olma ihtimali çok yüksektir. Bu konuda benzer çalışmalar yapılmış DNS sorgularının çok fazla akış yaparken veri miktarının küçük olduğu gösterilmiştir [21]. Bu bulgu Tablo 3'de de doğrulanmaktadır. Diğer yandan 1024 Byte'dan büyük paketlerin büyük bir kısmının yine Tablo 3'den de görülebileceği üzere HTTP protokol verisi olduğu tespiti yapabilir.

Kullanıcılara gelen ve giden IP paketlerinin yükü (payload) Tablo 2'de de gösterildiği gibi maksimum iletim birimi (MTU) boyutunda olduğundan bölünme görülmemektedir.

Tablo 2: **IP Türüne Göre Trafik**

Ağ Katmanı Türü	Veri Boyutu	Yüzdesi (%)
IP Trafiği	123.1 GBytes	99.9
Fragmented IP	82.7 MBytes	0.1
IP olmayan Trafik	988.9 KBytes	0

Atlama sayısı (HOP Count) İnternetteki iki nokta arasındaki geçiş noktalarının sayısını ifade etmektedir. Bu sayı ne kadar fazla ise iki uç arasında sorun yaşanma olasılığı da o kadar da artmaktadır. Şekil 3'de verilerin atlama uzaklıklarının yüzdelik dağılımı verilmiştir. 12 ile 20 atlama noktası arası tüm trafiğin %76'sını oluşturmaktadır. Türkiyedeki bir uca Kuzey Kıbrıstan ulaşabilmek için ortalama 8-12 atlama noktasından geçmek gerekmektedir. 12-20 atlama noktası ise trafiğin yabancı kaynaklı sitelere yoğunlaştığını göstermektedir.



Şekil 3: **Atlama sayılarının yüzdelik dağılımı**.

Tablo 3'de TCP ve UDP protokollerininin port numaralarına göre trafik ve akış verileri gösterilmektedir. Bu tabloda HTTP trafiğinin %43 gibi bir oranda olduğu ve akış başına ortalamasının da 415 kByte gibi bir miktarda olduğu görülmektedir. Bu da HTTP trafiğinde çoklu ortam nesnelerinin yani video, ses yada büyük resim öğelerinin bulunduğunun bir göstergesidir. Bu tespit Ntop programının başka bir analiz kısmımında doğrulanmaktadır. ADSL kullanıcılarının youtube ve facebook gibi yoğun trafik yaratan sitelere erişim yaptığı tespit edilmiştir. Ayrıca sistem, virus programları güncellemelerinin'de bu trafikte payları olduğu görülmüştür.

Yine Tablo 3'de DNS paketlerinin veri büyüklükleri az olmasına rağmen akış sayılarının fazla olması dikkat çekicidir. Bu ise önceden bahsettiğimiz DNS sorgularını ifade etmektedir.

Diğer paketler ise Ntop tarafından analiz edilemeyen büyük ihtimalle P2P trafiğini gösteren kısımdır. P2P trafiği bilinen port numaraları dahilinde toplam veri miktarında sadece %2'lik bir pay almaktadır. Ancak akış miktarlarına bakıldığında %77'lik kısım diğer port numaralarında yoğunlaşmıştır. P2P sistemlerinin doğası gereği uçlar birbirlerine yüzlerce noktadan bağlanabilmektedir. Bu da %54 trafiği oluşturan kısmın P2P ait olduğunu göstermektedir.

Tablo 3: **TCP/UDP protokol dağılımı**

TCP/UDP Protokol	Veri(kB)	Akış	Akış Ort(kB)	Veri (%)	Akış (%)
FTP	912	121	7,54	0,001	0,002
HTTP	56098816	134901	415,85	43,749	1,675
DNS	233984	1506922	0,16	0,182	18,707
Telnet	60	13	4,62	0,000	0,000
NetBios	1400	11004	0,13	0,001	0,137
Mail	1048576	50124	20,92	0,818	0,622
SNMP	210	1886	0,11	0,000	0,023
VoIP	2300	20966	0,11	0,002	0,260
SSH	250	1304	0,19	0,000	0,016
Gnutella	3900	2796	1,39	0,003	0,035
Kazaa	3900	20	195,00	0,003	0,000
edonkey	60000	3379	17,76	0,047	0,042
Bittorrent	320000	21397	14,96	0,250	0,266
Messenger	200000	99842	2,00	0,156	1,239
Diğer	70254592	6200762	11,33	54,788	76,976
Toplam	128228900	8055437			

Diğer portlar ise kayda değer bir trafik yada akış yaratmamışlardır.

4.2. Trafik Verileri Üzerinde Saldırı Analizi

Trafik verileri üzerinde Snort imzalarının 28 Eylül 2009 tarihli veritabanını kullanarak aşağıda verilen sonuçlara ulaşılmıştır.

Tespit edilen anormalik ve saldırı sayısı: 33269

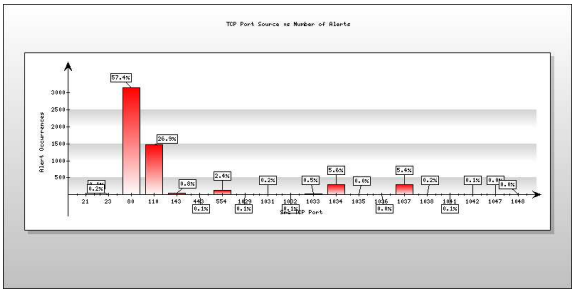
Tekil olarak tespit edilen saldırı sayısı: 45

Saldırıların gerçekleştiği tekil IP miktarı: 2546

Tablo 4: **Sınıflandırılmış saldırı türlerinin yüzdelik dağılımı.**

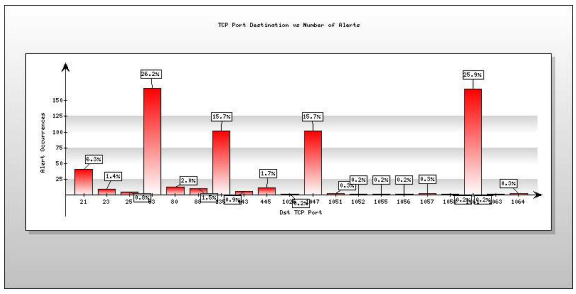
Saldırı Sınıfı	Yüzde(%)
Kural ihlali	58
Sınıflandırılmamış	18
Shell kodu	15
Admin yetkisi alma saldırısı	3
Gizli aktivite	3
Kullanıcı yetkisi alma saldırısı	2
Trojan	1

Tablo 4'de sınıflandırılmış saldırı türlerinin yüzdelik dağılımı verilmiştir. Burdaki tabloda kural ihlallerinin en fazla yüzde ile tespit edildiği gösterilmektedir. Kural ihlalleri genelde protokollerin tanımlanmış davranışları dışında gerçekleşen aktiviteleri ifade eder. Trafik içinde bu soruna açan paketler incelendiğinde bunun P2P veri transferi olduğu tespit edilmiştir. Sınıflandırılmamış olan saldırılar ise ftp transferinin kriptolanarak yapılması olarak tespit edilmiştir. Shell kodu olarak 3. en fazla görülen saldırı ise POP3 protokolünde gönderilen işlem yapma kodu olduğu tespit edilmiştir. Diğer saldırılar ise klasik trojan ve virus saldırılarını göstermektedir. Burdaki veriler ışığında yanlış uyarı alma ihtimalinin çok yüksek olduğu görülmektedir.



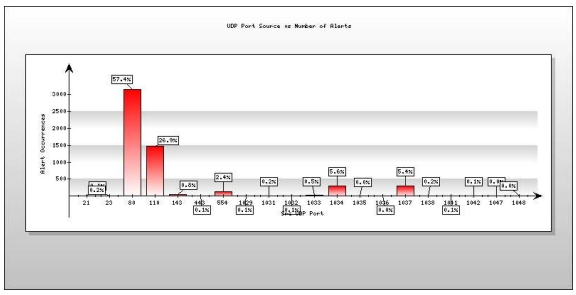
Şekil 4: **TCP kaynak portuna göre saldırı sayıları.**

Şekil 4 ve 5'de TCP kaynak ve hedef portlarına yada portlarında tespit edilen anormalik oranları gösterilmektedir. TCP kaynak portundan %57 ile 80 porttan ve %26 ile POP3 bunu izlemektedir. Ayrıca 1034 ve 1037 portlarda da uyarı alınmıştır. TCP hedef portlarında %53 ile DNS portunda alınan uyarılar ve 135,1047, 1061 portlarından alınan uyarılar görülmektedir. DNS sorgulama için UDP protokolü kullanmasından dolayı bunun bir saldırı denemesi olması muhtemeldir. Diğer portlar ise Microsoft firmasının işletim sistemlerinde açık bulmak için deneme yapan uygulamalardır.

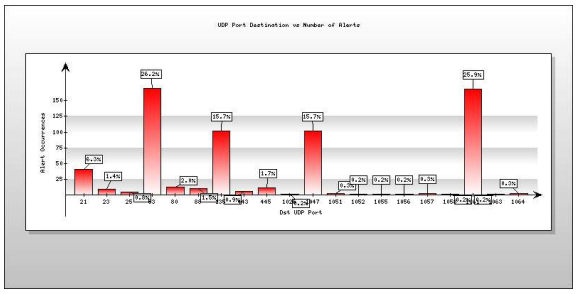


Şekil 5: **TCP hedef portuna göre saldırı sayıları.**

Şekil 6 ve 7'de UDP protokolü üzerinde yapılan kural ihlalleri gösterilmiştir. UDP protokolü ile 80 ve 110 portları kullanımı yine şüheli bir durumdur. Bunların port taraması olma ihtimali büyüktür. Hedef portlarında 53,135,1047 ve 1061 yine benzer şekilde virus yada trojan aktivitelerini göstermektedir.



Şekil 6: **UDP kaynak portuna göre saldırı sayıları.**



*Şekil 7***: UDP hedef portuna göre saldırı sayıları.**

5. Sonuç

Bu çalışmada, Kuzey Kıbrıstaki geniş bant kullanıcılarının bir kısmının erişim verileri kullanılarak, ağ üzerindeki davranışları analiz edilmiştir.İnternet trafik akışlarında beş yıl içinde dramatik değişiklikler olmuştur. Şu anda İnternet trafiği daha çok P2P ve çoklu ortam erişimleri üzerine yoğunlaşmaktadır. Benzer davranışların analiz edilen veriler üzerinde de olduğu gösterilmiştir. Bu da ileride geniş bant İnternet erişimi olan kullanıcıların, daha da fazla bant genişliğine ihtiyacı olacağını göstermektedir. Bir başka tespit ise, Kuzey Kıbrıstaki geniş bant kullanıcıların İnternet servislerine çoğunlukla Amerika yada Avrupa kaynaklı sunuculardan ulaştığı gözlemlenmiştir. Bunun nedeni de Türkçe dilinde yada Türkiye'den servis veren sitelerin yeterli hizmet sunamaması yada tercih edilmemesi olarak verilebilir.

Saldırı analizinde ise, geniş bant kullanıcılarının genelde Trojan yada virus yayılma saldırılarına maruz kaldıkları gözlemlenmiştir. Gelen saldırıların büyük bir kısmı Microsoft sistemi açıklarını kullanmaya çalışmaktadır. Bunların kaçının başarılı olduğu şu anda bilinmemektedir. Ancak ADSL modemler yada bilgisayarlar üzerindeki güvenlik duvarları bu tür saldırıların engellenmesine yardımcı olmaktadır.

6. Teşekkür

Bu çalışmada verilerin toplanması aşamasında yazara destek ve imkan veren Mehmet Alptürk'e teşekkür ederiz.

Ayrıca Kuzey Kıbrıs Türk Cumhuriyeti Milli Eğitim Bakanlığına sağladıkları makina ve techizat desteğinden dolayı teşekkür ederiz.

7. Kaynakça

[1] The World in 2009: ICT Facts and Figures, http://www.itu.int/ITU-D/ict/material/Telecom09_flyer.pdf, 2009

[2] K.C. Claffy. Internet Traffic Characterization. PhD thesis, University of California, San Diego, 1994.

[3] D.E. Denning, "An Intrusion Detection Model", IEEE Transactions on Software Engineering, SE-13:222-232, 1987.

[4] N. J. Puketza, K. Zhang, M. Chung, "A Methodology for Testing Intrusion Detection Systems", IEEE Transactions on Software Engineering, Volume 22, Issue 10, pp. 719 – 729, 1996.

[5] Novikov, D. Yampolskiy, R.V. Reznik, L., "Anomaly Detection Based Intrusion Detection", ITNG 2006, pp. 420-425, 2006.

[6] Tcpdump, http://www.tcpdump.org/tcpdump_man.html

[7] Jain, R., Routhier, S. A., "Packet Trains and New Model for Compter Network Traffic", IEEE Journal of Selected Areas Communications, (1986).

[8] Larson, R., Farber, B., "Elementary Statistics Picturing the World 2nd ed.", Prentice Hall, 189 (2003).

[9] Feldmeier, D. C., "Improving Gateway Performance With A Routing-Table Cache", IEEE INFOCOM, (1988).

[10] Mogul, J. C., "Network Locality at the Scale of Process", Digital Equipment WRL Research Report 91/11, Kasım (1991).

[11] Broido, A., Hyun, Y., Claffy, K., "Their share: diversity and disparity in IP traffic", Presented at the PAM workshop , (2004).

[12] Reed, W. J., "The Pareto, Zipf and other power laws", Economics Letters, 74:(1): 15-19 (2001).

[13] S. S. Kim, A. L. N. Reddy, "Statistical Techniques for Detecting Traffic Anomalies Through Packet Header Data", IEEE/ACM Transactions on Networking, vol.16, pp. 562-575, June 2008.

[14] A. Lakhina, M. Crovella, C. Diot, "Characterization of Network-Wide Anomalies in Traffic Flows", in Proc. 4th ACM SIGCOMM conference on Internet measurement, Taormina, pp. 201-206, 2004.

[15] D. Katz, R. Saluja, Three-Way Handshake for Intermediate System to Interm, IETF RFC 3373, 2002

[16] IPv4 Global Unicast Address Assigments, http://iana.org/assigments/ipv4-address-space
[17] B. Mukherjee L.T. Heberlein and K.N. Levitt, "Network Intrusion Detection," IEEE Network, pp. 26-41, May 1994.
[18] Martin Roesch, “Snort - Lightweight Intrusion Detection for Networks” , Proceedings of the 13th USENIX conference on System administration, November 07-12, 1999
[19] Deri L. , Suin S., “Effective traffic measurement using ntop”, Communications Magazine, IEEE, pp. 138 - 143 Volume: 38 , Issue: 5, May 2000
[20] Basic Analysis and Security Engine, http://base.secureideas.net/
[21] Thompson, K. Miller, G.J. Wilder, R. , Wide-area Internet traffic patterns and characteristics , Network, IEEE V:11, On page(s): 10-23, Nov/Dec 1997