

Pasif Ağ Verileri Üzerinden Düzensizlik Tespiti

Devrim SERAL, Beyhan ÇALISKAN

Abstract—Through the history, people have used several different ways to communicate. Over the few decades, Internet has become the primary source of information and important media for communication. This makes the sustainability of Internet crucial. On the other hand, the problems encountered on networks of various sizes that make up the Internet can seriously effect the performance of Internet. These problems usually originate from the anomalies of the networks and the immediate detection of anomalies in high capacity networks is a very resource consuming effort. This paper focuses on methods for anomaly detection which will require less resources by making use of netflow data.

Keywords — Site security monitoring, Networks, Computer Network Security

Özet—İnsanoğlu çağlar boyu bilgi edinmek ve haberleşmek için değişik yöntemlere başvurmuştur. Günümüzde ise İnternet, hem bilgi edinmek hemde haberleşmek için kullanılan en önemli araçlardan biri haline gelmiştir. Bu yüzden İnternetin sürekliliği büyük önem taşımaktadır. İnterneti meydana getiren değişik büyüklükteki ağlar üzerinde meydana gelen sorunlar, İnternete erişimi etkileyebilmektedir. Ağlar üzerinde meydana gelen sorunlar, genelde ağ düzensizliklerinden kaynaklanmaktadır. Yüksek hızlı ağlarda, anlık düzensizlik tespiti yapmak çok fazla kaynak gerektiren bir işlemdir. Bu çalışmada daha az kaynak gerektiren pasif ağ verileri kullanarak düzensizlik tespiti yapma yöntemleri ele alınacaktır.

Anahtar Kelimeler— Ağ güvenliği, Bilgisayar Ağ Güvenliği, Düzensizlik Tespiti

I. GİRİŞ

Ağ sistemlerine erişim, donanımsal nedenlerin dışında ağ köttöye 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 [1]. Ağ saldırı tespit sistemleri, imza tabanlı ve düzensizlik tabanlı olarak sınıflandırılabilirler [2]. İmza tabanlı sistemler, bilinen saldırı türlerine göre yazılan kurallar ile çalışırlar [3]. Ancak bu sistemlerde yeni saldırılar için gerekli olan kurallar, sadece güvenlik uzmanları tarafından güncellenebilmektedir.

Devrim Seral, Uluslararası Kıbrıs Üniversitesi, Mühendislik Fakültesi, Bilişim Sistemleri Mühendisliği, Lefkoşa-Kıbrıs'ta öğretim görevlisidir. (e-mail: dseral@ciu.edu.tr)

Beyhan Çalışkan, ULAKBİM, Ankara'da sistem yöneticisi olarak çalışmaktadır (e-mail: beyhan@ulakbim.gov.tr)

Bu durum, imza tabanlı sistemleri sıfır gün saldırıları (zero day attack) karşısında etkisiz bırakabilmektedir [4]. İmza tabanlı sistemler, analiz sırasında paket verisinin tümünü kullanmak zorundadırlar. Bundan dolayı yüksek hızlı ağlarda performansı azaltıp maliyeti artırdığından çok fazla tercih edilmezler. Gelişen teknoloji ile ağ hızları Gbps seviyelerine ulaşmış ve imza tabanlı sistemler yerine düzensizlik tabanlı sistemler önem kazanmıştır [5]. Düzensizlik tespiti için güvenlik uzmanları tarafından yazılmış kurallara gereksinim duyulmaz ve yeni saldırı türleri tespit edilebilir. Ancak bu tür sistemler, paket verileri (payload) ile ilgili olmadıkları için saldırıların özelliklerine ait bilgiler veremezler ve imza tabanlı sistemlere göre hatalı uyarı (false alarm) verme ihtimalleri daha fazla olabilmektedir.

Bu makalede, pasif ağ verileri üzerinden düzensizlik tespiti yöntemleri verildikten sonra örnek akış verisi üzerinde uygulaması anlatılacaktır. Pasif ağ verileri akış veri standardı olan NetFlow [6] formatında yönlendirici üzerinden alınacaktır. NetFlow, IP trafiğini özelliklerine göre ayırabilmekte, kaynak adresi, varış adresi, süre ve port bilgilerini detaylı şekilde verebilmektedir. Bu özellikler, ağ saldırılarından kaynaklanan düzensiz trafiği tespit etmekte kullanışlı olmaktadır. Makalenin ilk bölümünde düzensizlik tespitinde istatistiksel yöntemler incelenmiş, ikinci bölümünde ise yapay sınır ağları ile düzensizlik tespiti yöntemleri değerlendirilmiştir. Son bölümde Ulusal Akademik ağ trafiğinden alınan örnek verilerden yararlanarak saldırı tespiti yapılmıştır.

II. DÜZENSİZLİK TESPİTİNDE İSTATİSTİKİ YÖNTEMLER

Ağ trafiğinde oluşan düzensizliği inceleyerek, saldırı tespit etmek için değişik çalışmalar yapılmıştır. Bu çalışmaların birçoğunda istatistiki yöntemler ve trafik örnekleme (sampling) kullanılarak sonuç elde edilmeye çalışılmıştır [7],[8]. Yönlendiricilerden toplanan akış verileri (flow) ve ip paket başlıkları bu araştırmaların temelini oluşturmaktadır. Her iki yöntemde de paketlerin veri kısmına bakılmaksızın yönlendirme bilgisi, kaynak adresi, varış adresi, kaynak portu, varış portu, aktarılan veri büyüklüğü (byte) gibi bilgilerden faydalanarak modellemeler yapılmıştır [9]. Bu makalede akış verileri kullanılarak düzensizlik tespiti yöntemleri irdelenmiş ve istatistik yöntemler genel olarak iki başlık altında toplanmıştır; *En Çok ve Baz Değer, İz Eşleştirme*.

A. En Çok ve Baz Değer

Baz değer, geçmişte kaydedilen ağ trafiğine göre oluşturulmuş şablondur. Bu şablon normal ağ trafiğini temsil eder. Ağ trafiğinde meydana gelen ve baz değerden farklı olan her türlü trafik düzensiz olarak kabul edilir. Düzensiz trafiğin incelenmesinde kullanılan genel yöntem akış içerisindeki değişimleri tespit etmektir. Belirli bir zaman diliminde en fazla değişimi tespit etmek *en çok* yöntemi olarak tanımlanmaktadır.

En çok yönteminde, meydana gelen düzensizlikleri tespit ederken iki ayrı yöntem izlenebilir. En çok oturma yönteminde; belirli bir zaman dilimindeki oturma sayısı (session) temel alınır. En çok veri yönteminde ise; belirli bir zaman diliminde aktarılan veri miktarı (byte) temel alınır.

En Çok Oturma

Belirli bir istemci veya sunucuya ait ağ trafiğinde meydana gelen ani oturma sayısı artışı DoS/DDoS, solucan aktivitesi, ağ taraması gibi birçok sebepten kaynaklanabilir. En fazla oturma sayısının açıldığı sunucu veya ağ'daki oturma sayısı ile baz değer karşılaştırılınca olası saldırı tespit edilebilir.

Ağdaki herhangi bir bilgisayar servis bağlantısı yaparken kabul edilebilir sıklıkta oturma açar. Eğer oturma sayısında çok hızlı ve ani artışlar gözleniyorsa, bilgisayarın bir solucan tarafından etki altına alındığı ve başka bilgisayar veya ağlara doğru yayılmaya çalıştığı söylenebilir. Solucanların ağdaki faaliyetleri, konak bilgisayardan diğer kurbanları ararken ağı normal ağ karakteristik yapısında farklılıklar oluşturur. Bu farklılık akış verilerindeki artıştan tespit edilebilir.

Bir diğer durum ise belirli bir sunucu veya ağa yönelik akış sayısındaki ani artıştır. Genellikle bu tür artışlar servis veren sunuculara yöneliktir. DoS/DDoS saldırıları servis veren sunucu veya ağı karakteristik yapısını değiştirdiği için yine akış verileri yardımıyla saldırı tespit edilebilir.

En Çok Veri

Sunucu veya istemcilerin belirli bir zaman diliminde bant genişliğini hızlıca tüketmeleri normal bir durumu değildir. Düzensiz trafiği analiz etmek için bu konuda çalışmalar yapılmıştır [10]. Baz değerden farkı açıkça gözlenebilen bu tür trafiğin kaynağı yine solucan veya servis engelleme saldırıları olabilmektedir. Bu saldırıları tespit etmek çok kolay olmakla birlikte hatalı uyarı alma ihtimali daha fazladır. Bunun nedeni yedekleme veya dosya transferi gibi uygulamalardan kaynaklanan ve ağ trafiğinde oluşan ani ve yüksek veri akışları sayılabilir.

B. İz Eşleştirme

İz eşleştirme, normal dışı trafiğin tespit edilmesinde bir diğer 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 [11] 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 değerinin 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 [12] gelen trafik düzensiz olarak değerlendirilebilir. Ayrıca ağa ait fakat kullanılmayan ip adreslerine doğru yapılan trafik ağ taraması veya solucan aktivitesini işaret edebilir. IP veritabanı örnekleme dışarıdan gelen saldırılara karşı etkili olabildiği gibi aynı yaklaşımla iç ağdan yapılan saldırıların da tespitinde önemli rol oynayabilir.

III. YAPAY SİNİR AĞLARI İLE DÜZENSİZLİK TESPİTİ

Ağlar üzerinde oluşan düzensizlikleri tespit etmek için yapay sinir ağlarını kullanmak bir diğer yöntemdir. Bu sistemler yapay sinir ağlarının, önceden kaydedilmiş problem oluşturan düzensizlik verileri yardımıyla eğitilmesine dayanır [13]. Bu sistemler hem yanlış kullanım hemde düzensizlik tespit sistemleri ile birlikte anılır.

Yapay sinir ağlarının Çok katmanlı Algılama (Multilayer Perception) [14] ve Kendinden Teşekküllü Haritalar (Self-organizing Map) gibi farklı yaklaşımları da kullanılmaktadır [15].

Yapay sinir ağlarında Kendinden Teşekküllü Haritalar (KTH) öncelikle normal davranış gösteren ağ trafiğini öğrenme periyodundan geçirdikten sonra düzensizlik hareketlerini tespit edebilmektedir. Ancak bu sistemin en büyük kısıtlaması neron sayısının ağ performansını etkilemesidir. Çıkış düğümlerinin sayısını artırmak haritanın çözünürlüğünü artırmakla beraber veri işleme süresi dramatik bir biçimde artırmaktadır.

Yapay sinir ağları, ağ saldırı tespitinde kullanılırken bir diğer sorunu da zaman gecikmeli saldırıları tespit edememesidir [16].

Tüm yöntemlerde istenen yanlış uyarı miktarını mümkün olduğunca aşağıya çekmektir.

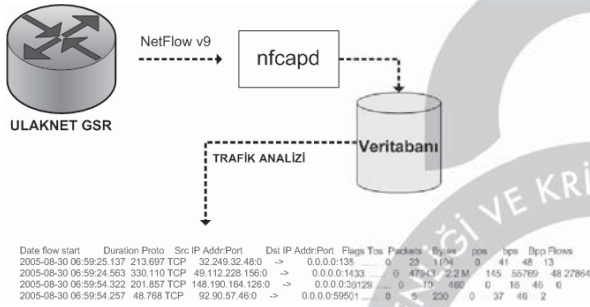
IV. AKADEMİK AĞDA DÜZENSİZLİK TESPİTİ

ULAKNET; Türkiye'deki tüm akademik kurumları, Türk Tarih Kurumu, Milli Kütüphane, YÖK, ÖSYM, TÜBİTAK, Türkiye Atom Enerjisi Kurumu ve Türk Silahlı Kuvvetleri'nin Ar-Ge birimlerinden oluşan geniş bir ağa hizmet sunmaktadır. Bu uçlarda bulunan yaklaşık 89300 öğretim görevlisi, araştırmacı ve 2.000.000 üzerinde üniversite öğrencisinin İnternet bağlantısı ULAKBİM tarafından sağlanmaktadır [17].

A. Yöntem

Düzensizlik tespiti için ULAKNET ağında alınan bir aylık akış verisi üzerinde çalışılmıştır. Akış verileri, 3Gbps bant genişliğine sahip akademik ağın ana omurga yönlendiricisi üzerinden Cisco NetFlow v9 standardında alınmıştır. Şekil 1'de gösterildiği gibi, akış şemaları, açık kaynak kodlu nfcapd [18] yazılımı ile toplanmış ve verilerin hızlı işlenmesi için Perl [19] betikleri yardımıyla MySQL [20] veritabanına kaydedilmiştir.

ULAKNET ağında düzensizlik tespiti için kullanılan yöntemler makalenin birinci bölümünde anlatılan istatistik temelli yaklaşımlara dayanmaktadır. Bu çerçevede deneyler en çok yöntemi ve iz eşleştirme olarak iki başlık altında toplanmıştır. Yapılan çalışma saldırı şüphesi olan trafiği ağ ve sistem yöneticileri tarafından görünür kılmaya yöneliktir [21]. Daha sonra gerekli modelleme yaklaşımları ile otomatik uyarılar üreten ve saldırıları engelleyen bir sistem geliştirilebilir.



Şekil 1. Netflow akış verilerinin alınması

En Çok Yöntemi Uygulaması

İnceleme yapılan bir aylık akış verisi 5, 10, 30 ve 60 dakikalık periyotlarla analiz edilmiştir. Farklı periyotlarda inceleme yapılmasının temel nedeni, en çok yönteminde saldırıların tespiti için bir eşik değer öngörülmesidir.

Deneyin ilk kısmında 5, 10, 30 ve 60 dakikalık zaman dilimleri kullanılarak akış verisi içerisinde en çok oturum açan istemciler tespit edilmiştir. Yapılan inceleme sonucu, analiz periyodu uzadıkça en çok akış yöntemine ait başarımın düştüğü hatta etkisiz kaldığı gözlemlenmiştir. Bu durumun nedenini araştırıldığında, 3Gbps gibi yüksek bir bant genişliğinde normal trafiğin şüpheli trafiğe göre daha fazla yer almasından kaynaklandığı tespit edilmiştir. Bu çerçevede en çok akış yöntemleri uygulanırken, kısa zaman dilimlerinde analiz yapmanın, anlık artışları ve düzensizliği tespit etmekte etkili olacağından hareket edilmiştir. Bu yüzden 5 dakikalık periyotlarla trafik analizi yapılmıştır. En çok oturum yöntemi uygulanarak tespit edilen bir düzensizlik aşağıda gösterilmiştir.

```
TCP 194.27.X.X:80 -> 20.95.31.62:1024 .A..S. 1 44 0 0 44 1
TCP 194.27.X.X:80 -> 3.110.217.64:3072 .A..S. 1 44 0 0 44 1
TCP 194.27.X.X:80 -> 85.255.5.60:3072 .A..S. 1 44 0 0 44 1
TCP 194.27.X.X:80 -> 138.163.116.123:1024 .A..S. 1 44 0 0 44 1
TCP 194.27.X.X:80 -> 35.53.251.68:1024 .A..S. 1 44 0 0 44 1
TCP 194.27.X.X:80 -> 44.77.161.38:3072 .A..S. 1 44 0 0 44 1
TCP 194.27.X.X:80 -> 181.46.18.16:3072 .A..S. 1 44 0 0 44 1
```

```
TCP 194.27.X.X:80 -> 176.116.55.102:1024 .A..S. 1 44 0 0 44 1
TCP 194.27.X.X:80 -> 201.208.253.34:1024 .A..S. 1 44 0 0 44 1
TCP 194.27.X.X:80 -> 122.121.178.35:1024 .A..S. 1 44 0 0 44 1
```

Örnek diyagram sırasıyla; protokol, kaynak ip ve kaynak port, hedef ip ve hedef port, tcp bayrağı, paket sayısı, paket büyüklüğü (byte), saniyedeki bit sayısı, paket başına byte ve oturum sayısını göstermektedir. En çok oturum yöntemi ile tespit edilen bu trafiğin normal olmadığı hemen görülebilmektedir. 194.27.X.X ip adresine sahip 80 numaralı porttan hizmet veren web sunucusu birçok farklı ip adresine SYN-ACK paketleri göndermekte ve hedef portları da sürekli 1024 ve 3072 olmaktadır (Sunucu adresi gizlenmiştir). Tespit edilen bu düzensizlik ilgili web sunucusuna yapılan SYN flood saldırısına aittir. En çok akış yöntemi, ağ trafiğinin karakteristik yapısında belirgin değişiklikler yapan, yukarıda incelediğimiz saldırıyı tespit edebilirken, aynı zaman dilimi içinde yer alan bir başka saldırıyı tespit etmekte başarısız olabilir. Bu varsayımın temelinde, yüksek bant genişliğinde düzensiz trafiği normal trafikten ayırt edecek paket ve akış sayısının çok fazla olması gerektiği düşüncesi vardır. Bu varsayımı doğrulamak için en çok akış yöntemine TCP filtreleri yazılmıştır.

Aşağıda verilen akış verileri bir önceki akış verileri ile aynı zaman aralığından elde edilmiştir. TCP bayrağında SYN paketi olan istemcilere, en çok oturum yöntemi uygulanarak elde edilen veriler, 193.140.X.X ip adresli istemciden kaynaklanan ve 135 port adresini hedef alan faaliyetleri tespit etmiştir. Bu faaliyetin bir solucan saldırısı olduğu hemen fark edilmektedir.

```
TCP 193.140.X.X:2907 -> 193.140.53.155:135 ....S. 1 48 0 0 48 1
TCP 193.140.X.X:2926 -> 193.140.53.164:135 ....S. 1 48 0 0 48 1
TCP 193.140.X.X:2934 -> 193.140.231.7:135 ....S. 1 48 0 0 48 1
TCP 193.140.X.X:2971 -> 193.140.177.80:135 ....S. 1 48 0 0 48 1
TCP 193.140.X.X:2978 -> 193.140.53.187:135 ....S. 1 48 0 0 48 1
TCP 193.140.X.X:2984 -> 193.140.53.190:135 ....S. 1 48 0 0 48 1
TCP 193.140.X.X:3007 -> 193.140.53.202:135 ....S. 1 48 0 0 48 1
TCP 193.140.X.X:3027 -> 193.140.53.212:135 ....S. 1 48 0 0 48 1
TCP 193.140.X.X:3030 -> 193.140.177.91:135 ....S. 1 48 0 0 48 1
TCP 193.140.X.X:3045 -> 193.140.53.221:135 ....S. 1 48 0 0 48 1
TCP 193.140.X.X:3061 -> 193.140.231.42:135 ....S. 1 48 0 0 48 1
TCP 193.140.X.X:3074 -> 193.140.231.49:135 ....S. 1 48 0 0 48 1
TCP 193.140.X.X:3077 -> 193.140.177.111:135 ....S. 1 48 0 0 48 1
TCP 193.140.X.X:3099 -> 193.140.53.232:135 ....S. 1 48 0 0 48 1
TCP 193.140.X.X:3104 -> 193.140.231.60:135 ....S. 1 48 0 0 48 1
TCP 193.140.X.X:3114 -> 193.140.231.65:135 ....S. 1 48 0 0 48 1
TCP 193.140.X.X:3127 -> 193.140.177.131:135 ....S. 1 48 0 0 48 1
TCP 193.140.X.X:3118 -> 193.140.231.67:135 ....S. 1 48 0 0 48 1
TCP 193.140.X.X:3147 -> 193.140.231.75:135 ....S. 1 48 0 0 48 1
TCP 193.140.X.X:3154 -> 193.140.53.252:135 ....S. 1 48 0 0 48 1
TCP 193.140.X.X:3161 -> 193.140.177.137:135 ....S. 1 48 0 0 48 1
```

Bir diğer en çok yöntemi olan paket büyüklüğüne göre düzensiz trafik tespiti ULAKNET akademik ağında başarısız olmuştur. Bu yöntemdeki motivasyon saldırıların bant genişliğini hızlıca doldurabileceği varsayımına dayanmaktadır. Fakat ULAKNET gibi çok uçlu ve yüksek bant genişliğine sahip bir ağda, normal trafik karakterinin fazla oluşu şüpheli trafiği en çok veri yönteminden gizleyebilmektedir. Bu yöntemin geniş süreli uygulamasından verimli sonuç

almamayınca daha önce en çok oturum yöntemi ile tespit edilen saldırıya ait zaman aralığı TCP filtreleri de kullanılarak taranmıştır. Elde edilen sonuçlar etkin düzensizlik tespiti için yeterli olmamıştır.

Bu yöntemin mevcut durumda kullanılabilmesi istatistik yöntemlerden daha çok yapay sinir ağlarıyla mümkün olabilir. Yapay sinir ağı eğitilip ULAKNET ağına bağlı her bir uç için baz değer veritabanı oluşturulabilir. Ağda baz değer üzerinde veri akışı gerçekleşirse düzensiz trafik tespit edilebilir. Daha önce de belirtildiği gibi bu yöntemin hatalı uyarı verme ihtimali yedekleme ve dosya transferi gibi sebeplerden dolayı yüksek olması beklenebilir.

İz Eşleme Yöntemi Uygulaması

ULAKNET ağına iz eşleme yöntemi ile düzensizlik tespit uygulaması, istatistik yöntemlerin en başarılısı olmuştur. Akış semalarından elde edilen veriler IANA tarafından rezerve edilen ip blokları ile karşılaştırılmıştır. Bu çalışmada IANA tarafından rezerve edilen ip adreslerinin, asla geniş alan ağlarında bulunmaması gerektiğinden yola çıkılmıştır. Bu varsayımı uymayan bütün trafik düzensiz olarak kabul edilir. Aşağıdaki diyagramlarda iz eşleme yöntemi ile tespit edilen şüpheli trafikler gösterilmiştir.

TCP 193.140.X.X:49960 -> 192.168.163.169:515S. 1 52 0 0 52 1
TCP 193.140.X.X:49969 -> 192.168.163.170:2191S. 1 52 0 0 52 1
TCP 193.140.X.X:49972 -> 192.168.163.170:81S. 1 52 0 0 52 1
TCP 193.140.X.X:49977 -> 192.168.163.172:515S. 2 100 0 88 50 1
TCP 193.140.X.X:49979 -> 192.168.163.172:2191S. 1 52 0 0 52 1
TCP 193.140.X.X:49984 -> 192.168.163.173:515S. 1 52 0 0 52 1
TCP 193.140.X.X:49986 -> 192.168.163.173:2191S. 1 52 0 0 52 1
TCP 193.140.X.X:49988 -> 192.168.163.173:443S. 1 52 0 0 52 1
TCP 193.140.X.X:49993 -> 192.168.163.171:2191S. 1 52 0 0 52 1
TCP 193.140.X.X:49995 -> 192.168.163.171:443S. 1 52 0 0 52 1

Diyagramdan açıkça görüldüğü üzere 193.140.X.X ip adresli istemciye gelen trafik IANA tarafından rezerve edilmiş 192.168.0.0/16 ağı kaynaklıdır. Bu akış şemasından, ip adresini değiştirmiş saldırganın port tarama saldırısı gerçekleştirdiği görülmektedir. Tespit edilen bir diğer şüpheli trafik ise aşağıdaki akış diyagramına aittir. Web sunucusuna yapıldığı ve servis engelleme amaçlı olduğu açıkça belli olan bu saldırı 0.0.0.0/8 ağ kaynaklı olarak gözükmektedir. Fakat bu ağ IANA tarafından rezerve edilmiştir ve iz eşleme yöntemi tarafından saldırı tespit edilmiştir.

TCP 193.140.X.X:5823 -> 0.39.15.0:80S. 1 48 0 0 48 1
TCP 193.140.X.X:2678 -> 0.39.15.0:80S. 1 48 0 0 48 1
TCP 193.140.X.X:35671 -> 0.39.15.0:80S. 1 48 0 0 48 1
TCP 193.140.X.X:12301 -> 0.39.15.0:80S. 1 48 0 0 48 1
TCP 193.140.X.X:62520 -> 0.39.15.0:80S. 1 48 0 0 48 1
TCP 193.140.X.X:32299 -> 0.39.15.0:80S. 1 48 0 0 48 1
TCP 193.140.X.X:38133 -> 0.39.15.0:80S. 1 48 0 0 48 1
TCP 193.140.X.X:35579 -> 0.39.15.0:80S. 1 48 0 0 48 1
TCP 193.140.X.X:27852 -> 0.39.15.0:80S. 1 48 0 0 48 1
TCP 193.140.X.X:56331 -> 0.39.15.0:80S. 1 48 0 0 48 1
TCP 193.140.X.X:19893 -> 0.39.15.0:80S. 1 48 0 0 48 1
TCP 193.140.X.X:14261 -> 0.39.15.0:80S. 1 48 0 0 48 1
TCP 193.140.X.X:14736 -> 0.39.15.0:80S. 1 48 0 0 48 1
TCP 193.140.X.X:12718 -> 0.39.15.0:80S. 1 48 0 0 48 1
TCP 193.140.X.X:52480 -> 0.39.15.0:80S. 1 48 0 0 48 1
TCP 193.140.X.X:58488 -> 0.39.15.0:80S. 1 48 0 0 48 1

TCP 193.140.X.X:28680 -> 0.39.15.0:80S. 1 48 0 0 48 1
TCP 193.140.X.X:23348 -> 0.39.15.0:80S. 1 48 0 0 48 1
TCP 193.140.X.X:9118 -> 0.39.15.0:80S. 1 48 0 0 48 1

V. SONUÇ

Günümüzde İnternetin kesintisiz olarak çalışması hayati önem taşımaktadır. Bunun nedeni ise artık birçok kurumun ve bireyin hızlı ve zahmetsizce işlerini İnternet üzerinden halledebilmesidir. Erişimin herhangi sebepten dolayı kesilmesi zaman, maliyet ve iş kayıplarına neden olabilmektedir.

İnternet'in donanım sorunları dışında başka nedenlerle kesintiye uğraması genelde ağlar üzerinde görülen düzensizliklerden kaynaklanmaktadır.

Bu çalışmada, yüksek hızlı ağlarda düzensizlik tespitinde kullanılan yöntemler ele alınmış ve ULAKBİM gibi büyük bir ağdaki verilerden yararlanarak, temel düzensizlik bulgularının nasıl tespit edileceği gösterilmiştir.

Bu çalışmaya yazılım tabanlı uygulamalar geliştirilerek daha kapsamlı bir sistem haline getirilebilir. Böyle bir sistemin anlık veri akışları üzerinde düzensizlik tespit edip uyarılar üretmesi bir sonraki çalışma konusu olabilir.

TEŞEKKÜR

Bu çalışmada bizlere ağ akış verilerini ve analiz yapabilmemiz için gerekli olan donanımı sağladığı için ULAKBİM'e teşekkür ederiz.

KAYNAKLAR

- [1] D.E. Denning, "An Intrusion Detection Model", IEEE Transactions on Software Engineering, SE-13:222-232, 1987.
- [2] 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.
- [3] Novikov, D. Yampolskiy, R.V. Reznik, L., "Anomaly Detection Based Intrusion Detection", ITNG 2006, pp. 420-425, 2006.
- [4] K. Wang, S. J. Stolfo, "Anomalous payload-based network intrusion detection", RAID, pp. 203-222, Sept., 2004.
- [5] B. Choi, S. Bhattacharyya, "Observations on Cisco Sampled Netflow", ACM SIGMETRICS Performance Evaluation Review, Volume 33, Issue 3, pp.18 – 23, 2005.
- [6] Cisco Netflow, http://www.cisco.com/en/US/products/ps6601/products_ios_protocol_group_home.html.
- [7] 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.
- [8] A. Lakhina, M. Crovella, C. Diot, "Characterization of Network-Wide Anomalies in Traffic Flows", in Proc. 4th ACM SIGCOMM conference on Internet measurement, Taormina, 2004, pp. 201-206.
- [9] G. Dewaele, K. Fukuda, P. Borgnat, P. Abry, K. Cho, "Extracting Hidden Anomalies using Sketch and NonGaussian Multiresolution Statistical Detection Procedures", in Proc. 2007 workshop on Large scale attack defense, Kyoto, 2007, pp. 145-152.
- [10] Matthew V. Mahoney, "Network Traffic Anomaly Detection Based on Packet Bytes", in Proc. ACM symposium on Applied computing, Florida, 2003, pp. 346-350.
- [11] D. Katz, R. Saluja, Three-Way Handshake for Intermediate System to Interim, IETF RFC 3373, 2002
- [12] IPv4 Global Unicast Address Assignments, <http://iana.org/assignments/ipv4-address-space>
- [13] J. Z. Lei, A. Ghorbani, "Network Intrusion Detection Using an Improved Competitive Learning Neural Network", Communications Networks and Services Research Conference, pp. 190 - 197,2004.

- [14] A. K. Ghosh , A. Schwartzbard. "A study in using neural networks for anomaly and misuse detection", In Proceedings of USENIX Security Symposium, 1999.
- [15] B. C. Rhodes, J. A. Mahaffey, and J. D. Cannady, "Multiple self-organizing maps for intrusion detection", In Proceedings of the 23rd National Information Systems Security Conference, 2000.
- [16] Y. Yaho, Y. Wei, F. Gao, G. Yu, "Anomaly Intrusion Detection Approach Using Hybrid MLP/CNN Neural Network", ISDA'06, pp. 1095-1102, 2006
- [17] ULAKNET, <http://www.ulakbim.gov.tr/hakkimizda/tarihce/ulaknet>
- [18] nfdump, <http://nfdump.sourceforge.net>
- [19] Perl, <http://www.perl.org>
- [20] MySQL, <http://www.mysql.com>
- [21] G. Conti, K. Abdullah, "Passive Visual Fingerprinting of Network Attack Tools", in *Proc. ACM workshop on Visualization and data mining for computer security*, Washington, 2003, pp. 45-54.

