P2P ile YAŞAMAK

Murat Soysal
ULAKBİM
msoysal@ulakbim.gov.tr

Vedat Fetah
Ege Üniversitesi
BİTAM Kampüs Nw Yön. Grb.
vedat.fetah@ege.edu.tr

Gökhan Akın
İTÜ BİM
akingok@itu.edu.tr

Ar.Gör.Enis Karaarslan
Ege Üniversitesi
BİTAM Kampüs Nw Yön. Grb.
enis.karaarslan@ege.edu.tr

ÖZET

P2P, paylaşıma getirdiği hız, güvenilirlilik ve verim açısından çok yararlı bir protokoldür. Yalnız bu protokolün aşırı ve kontrolsüz kullanımında, oluşan bağlantılar ağ sistemlerinde yoğunluluk ve ona bağlı yavaşlamaya yol açmakta, band genişliğinin olması gerekenden fazla kullanılmasına yol açmaktadır. Paylaşılan dosyaların çoğunluğunun telif hakkına tabi olması ve bu tip bir paylaşımın hukuka uygun olmaması da ciddi bir sorundur. Bu nedenlerden dolayı, P2P protokolünü ve bu protokolü kullananları kontrol altında tutmamız gerekmektedir.

Bu çalışma, ULAKNET ağının daha verimli olarak kullanılması için yaptığımız araştırmaların özetidir. P2P protokolü, tespiti ve kısıtlanma yöntemleri detaylı olarak ele alınmış ve çözüm önerileri verilmiştir.

ABSTRACT

P2P, is a useful protocol as it speeds up sharing, is reliable and efficient. In the case of excessive and uncontrolled use, the connections cause intensity and slowdown in network systems and cause usage of more bandwidth then it should. Most of the shared files are copyrighted and this type of sharing is not legal. For these reasons, P2P protocol usage and the users of this protocol must be under control.

This study is a summary of the research which is done to use ULAKNET network more efficient. P2P protocol, detection and restriction methods are explained in detail and solution suggestions are given.

Anahtar Kelimeler: Ağ yönetimi, kampüs ağları, P2P, P2P engelleme, P2P kısıtlama, QoS, IDS, IPS

1.GİRİŞ

P2P (Peer to Peer)'i özetle bilgisayar kaynaklarının karşılıklı paylaşımı olarak tanımlayabiliriz. Kaynak paylaşımı, bilgi teknolojilerinin temel amacı olduğundan, buna hizmet eden her türlü protokol bizler için değerli olmalıdır. Bunlara ek olarak P2P, paylaşıma getirdiği hız, güvenilirlilik ve verim açısından çok yararlı bir protokoldür. Kontrol altına alındığında, telif hakkına tabii olmayan dosyaların paylaşımı için kullanımı yararlı ve gereklidir. Bu konuda öncelikle P2P'in ne olup ne olmadığı hakkında kendimize bazı sorular sormamız gerektiğini düşündük:

P2P gerçekten istenmeyen bir trafik midir?

P2P protokolünün yıllar içinde yaşadığı evrim sonucunda ortaya çıkan son hali, geleneksel sunucu-istemci iletişiminin yaşadığı bir çok dar boğazın aşılmasına yardımcı olmuştur. Bu anlamda düşünüldüğünde, P2P iletişimi çok yararlı ve istenen bir trafiktir. Ancak bu iletişim protokolünü yaygın hale getiren ve günümüzdeki kullanımının %90 civarında bir miktarını oluşturan uygulama, müzik ve film dosyalarının paylaşımıdır. Bu dosyaların büyüklüğü 3 MB ile 4,5 GB arasında değişmektedir. Bu büyüklükteki dosyalarını P2P gibi aynı anda bir çok kaynaktan indirmeye olanak sağlayan bir protokol ile paylaşılması, mevcut hat kapasitelerini sömürmektedir. Tek bir protokolün hattın kullanım oranının %60'lara varması, özel durumlar hariç ağ yöneticileri tarafından kabul edilemez bir durum oluşturmaktadır.

P2P ağında paylaşılan dosyaların büyük bir çoğunluğunu müzik ve film dosyaları oluşturmaktadır. Ayrıca genellikle telif hakkına tabi işletim sistemleri ve diğer yazılımlarda paylaşılan dosyalar arasında yer almaktadır. İndirilen trafiğin yanı sıra gönderilen trafiğin daha çok olması, üniversite ağının bir tür warez/korsan film kaynağı haline gelmesinin bir işaretidir. Bu konuda hukuksal bazı sorunların çıkması da muhtemeldir. Paylaşılan dosyaların çoğunluğunun telif hakkına tabi olması ve bu tip bir paylaşımın hukuka uygun olmaması, P2P protokolünü ve bu protokolü kullananları kontrol altında tutmamızı gerektirmektedir. Sonuç olarak P2P istenmeyen değil, hat kullanımı ve kullanıcıları ile kontrol altında tutulması gereken bir protokoldür.

P2P in gerçekten de akademik/kurumsal bir amaçla kullanılması mümkün müdür?

Bu konuda tüm dünyada şiddetli tartışmalar

yaşanmaktadır. P2P'in paylaşım konusunda getirdiği imkanların elektronik kitap, makale, eğitim amaçlı video ve müzik, GPL ile dağıtılan yazılımlar ve bilgisayar kaynağı paylaşımı gibi alanlara kanalize edildiğinde akademik amaca hizmet etmesi mümkündür. Ancak Napster ile yaygınlaşan P2P kullanımında bu akademik amaca hizmetin %5'lerin üstüne çıkması beklentiler dahilinde değildir.

Akademik/kurumsal ağın, akademik/kurumsal olmayan bir amaçla kullanılması ne kadar uygundur?

Bu konuda yapılacak yorumlarda oldukça dikkatli olmak gerekmektedir. Çünkü, ağ üzerinde akan trafiğin akademik ya da akademik olmayan olarak sınıflandırılması için elimizde çok geçerli bir yöntem yoktur. Türkiye ulusal akademik ağına bakıldığında, global internet çıkışlarını oluşturan TTNet bağlantılarının gün içindeki doluluk oranı %90'lara ulaşırken, Avrupa akademik ağı Geant'a olan bağlantının doluluk oranı %5 oranında kalmaktadır. Bu oranlar, ulusal akademik ağımızın genel karakteristiğini gösterse de, daha kesin hatlarla yorum yapmak konusunda yanıltıcı olabilir.

Herhangi bir trafiğin akademik olmadığından emin olsak bile, akademik ağ üzerinden akmasında sakınca olmaması gerektiği düşünülebilir. Sonuçta bu trafiğin hedefi ya da kaynağı, akademik dünyanın üyeleridir. Akademik ağın bir görevi de bu üyelerin her anlamda güncel kalmalarını sağlamaktır. Ama tabii ki hattın sömürülmesinin ve diğer kullanıcıların erişim performanslarının düşmesinin engellenmesi gerekmektedir. P2P'in bilinçli kullanılmasının gerektiği aşikardır. Örneğin en büyük sorun, kullanıcıların dosya çekerken yarattıkları trafikten değil, onların makinalarından çekilen trafikten kaynaklanmaktadır. Oluşan yüzlerce-binlerce bağlantı yönlendirici ve güvenlik duvarlarında yoğunluk ve ona bağlı yavaşlamaya yol açmakta, band genişliğinin olması gerekenden fazla kullanılmasına yol açmaktadır. Bu aynı zamanda, akademik ağın bir tür korsan film ve korsan müzik kaynağı olarak da kullanılması ve bu nedenle de bir nevi itibar kaybına da yol açabilmektedir.

P2P engellemek/kısıtlamak için teknik ve idari olarak neler yapılabilir?

Bu konuda idari olarak yapılması gerekenler P2P protokolüne özgü bir uygulama getirmemektedir. Bu trafiğin bant genişliği kullanımının ve kullanıcılarının kontrol altında tutulması gerektiği bilinci ağ uzmanları arasında artırılmalıdır. Ayrıca bu ibare, üniversite ve araştırma kurumlarının kullanıcı politikalarında uygun bir şeklide yer almalıdır. P2P trafiğine katkı yaptığı ve bu trafikle telif hakkına tabii dosyaları dağıttığı tespit edilen kullanıcılar hukuki yaptırımlarla karşılaşacağından, bu faaliyetlerde bulunmasına yardımcı olan bilgisayarı ve ağa bağlantısını sağlayan üniversite ve araştırma kurumları kullanıcılarına sorumluluklarını belirtmeli, karşılıklı imzalanacak kullanım politikasını oluşturmalıdırlar.

P2P protokolüne ait trafiğin hat kapasitesi üzerindeki olumsuz etkisini kontrol altına almak için ağda teknik olarak yapılması gereken işleri üç ana başlık altında toplayabiliriz:

- Band kapatisinin kısıtlanması: Protokol bazlı bant kapasitesi limitlenebilir bir yapı oluşturulmasıdır.
- Mesai saatlerinde izin verilmemesi: Özellikle bandgenişliğinin kısıtlanamadığı durumlarda, kurum tarafından mesai saatlerinde P2P trafiğinin yapılması yasaklanabilir. İmza tabanlı çözümlerle P2P trafiği engellenebilir, hat istatistikleri aracılığıyla hattı sömürenler tespit edilip gerekli yaptırımlar uygulanabilir.
- Kayıtlama: Geçmiş zamanda yapılan bir P2P trafiği hakkında IP bazlı bir şikayet oluştuğunda, söz konusu IP'ye sahip bilgisayar ve kullanıcısının fiziksel olarak tespit edilebilmesidir.

2.P2P GELİŞİM SÜRECİ

Ağ trafiği içinden P2P protokolüne ait paketleri tespit edip, bu paketler için genelden farklı politikalar uygulamanın ilk şartı, P2P protokolü davranış şeklini iyi algılamaktır. Bu amaçla, bildirinin bu bölümünde P2P protokolünün tarih içinde geçirdiği evrim ve her yeni nesil P2P protokolü için geliştirilen belirleme yöntemlerinden bahsedeceğiz.

P2P protokolünün bugün ki kullanımıyla popüler bir uygulama olmasının temelleri, 1999 yılında Shawn Fanning tarafından ortaya çıkartılan Napster'a dayanmaktadır. Öncelikle amacı müzik dosyalarının rahat paylaşılması olan uygulamanın çalışma mantığı gayet basitti. Napster şirketi binasında tutulan sunucular, Napster yazılımını bilgisayarlarında çalıştıran tüm kullanıcıların paylaşıma açtığı dosyaların listelerini tutmaktaydı. Napster yazılımı ile arama yapan bir kullanıcının (istemci) isteği, protokole ait "kontrol paketleri" kullanılarak şirkette bulunan sunucuya ulaşıyor, sunucu da aranan dosya ismini tuttuğu listede arıyordu. Eğer dosyayı paylaşıma açmış bir kullanıcı var ise, listeden elde edilen sonuca göre bu kullanıcının IP adresi, istemciye yine "kontrol paketleri" kullanılarak iletiliyordu. Bir sonraki aşamada, istemci IP adresini bildiği kullanıcıdan istediği dosyayı "veri paketleri" kullanarak indirmeye başlıyordu. İnternet bağlantısının yaygınlaşması ve müzik dosyalarına ücretsiz sahip olabilme fırsatının çekiciliği sayesinde Napster

kullanımı hızla arttı. Ancak bu artış, müzik piyasası sağlayıcılarını rahatsız etti. 2000 yılında, Metallica müzik grubu ve Amerika Kayıt Endüstrisi Birliğinin (Recording Industry Association of America) açtığı davalar sonucunda Napster sunucuları mahkeme kararıyla kapatıldı.

İkinci nesil P2P protokolü olarak anılan Gnutella, Napster'ın çok kolay ve hızlı bir şekilde kapatılabilmesine fırsat veren tek sunuculu paylaşımına yenilikler getirmiştir. Herhangi bir Gnutella uygulama yazılımını bilgisayarına kuran bir kullanıcı, yazılımı çalıştırdığında otomatik olarak bir sunucuya bağlanmaktaydı. Bu sunucunun IP adresi, yazılımı programlayanlar tarafından başka bir sunucu bilgisi bilinmediğinde de paylaşımın sağlanabilmesi amacıyla yazılım içine gömülmüştü. Kullanıcı, istediği takdirde, bildiği başka Gnutella sunucu IP adreslerini yazılım veri tabanına ekleyebiliyordu. Yazılımı kullanarak dosya araması yapan istemcinin sorgusu, ilk olarak direk bağlı olduğu sunuculara aktarılıyordu. Sorguyu alan sunucu (kullanıcı), kendisinin ve kendisine direk bağlı diğer kullanıcıların paylaşıma açtığı dosya listesinde arama yapıyordu. Bir sonuca ulaşıldığında, dosya sahibinin IP adresi istemciye gönderiliyordu. Eğer arama başarısız olursa, sorgu sunucu tarafından kendisine direk bağlı olan tüm kullanıcılara (sunucu) aktarılıyordu. Daha önce yönlendiricilerde kullanılan ve "gossipping" (dedikodu) olarak anılan bu teknik sayesinde sorgu ağ içinde kademe kademe ilerleyebiliyordu. Sorgunun bir sunucudan kendisine direk bağlı sunuculara aktarılma işlemi sırasında istemci tarafından belirlenen TTL (Time-to-Live) değeri bir kademe düşürülüyordu. Bu değer sıfıra ulaştığında sorgu sona erdirilerek sonsuz döngünün önüne geçiliyordu. Arama sırasında her kullanıcının hem istemci hem de sunucu şeklinde davranıyor olması P2P iletişiminin geleneksel sunucu-istemci iletişiminden en önemli farkıdır. Napster'da bu fark sadece "veri paketleri iletişiminde" ortaya çıksa da Gnutella ile birlikte kontrol paketleri iletişimi de tüm kullanıcılar arasında yapılmaya başlandı. Gnutella trafiğin belirlenmesi ve engellenmesi konusunda Napster'a göre çok başarılı olsa da, sorgu sürecinin verimsizliği sebebiyle başarısız olmuştur.

Üçüncü nesil P2P protokolü Fast Track, arama yapmayı verimli hale getirme amacıyla ağda paylaşılan dosyaları indeksleme amaçlı çalışan ve sadece dosya sağlayan birçok sunucunun hizmet vermesi temeline dayanmaktadır. Supernode olarak adlandırılan bu sunucuların IP adresleri internet sayfalarında ve forumlarda anons edilmektedir. Uygulama yazılımını çalıştıran kullanıcı, bağlanacağı supernode'u seçerek sorgusunu başlatıyordu. Sorguyu alan sunucu kendisine bağlı kullanıcılarda dosya var ise hemen cevabı istemciye dönüyor, aksi durumda sadece diğer supernode'larla iletişime geçip sorguyu onlara yönlendiriyordu. Çok benzer bir protokol olan Direct Connect(DC), bu paylaşım mantığına kullanıcıların daha iyi iletişim kurabilmesi için "sohbet" özelliğini de eklemiştir. Bu özellik sayesinde DC kullanıcılarının diğer protokol kullanıcılarına göre daha sosyalleştiği, paylaşım mantığına insan varlığının katılmasıyla protokolün daha yaygın ve başarılı hale geldiği gözlenmiştir.

Son nesil P2P nesli olan BitTorrent ise atalarından çok farklı bir yöntem izlemektedir. Eski bir hacker olan Bram Cohen tarafından yazılan bu uygulamanın ilk adımı internette yapılacak bir arama sonrasında istenen dosyaya ait .torrent uzantılı dosyanın indirilmesidir. Yaklaşık 50 Kb büyüklüğünde olan bu dosya sayesinde, istemciler herhangi bir torrent yazılımı kullanarak bu dosyayı paylaşan kullanıcıların oluşturduğu kümeye (swarm) dahil olurlar. Bu kümedeki her kullanıcı dosyanın indirdiği kadarını diğer kullanıcılara sağlamakla yükümlüdür. Tüm bu işlemleri de izleyici (tracker) isimli bir sunucu kontrol eder. Bir kümenin kurulması için tüm dosyaya sahip en az bir kullanıcının (seeder) olması gerekir. Bu yapı dosyanın hızlı bir şekilde paylaşılmasını sağlar.

3. P2P TRAFİĞİNİN BELİRLENMESİ

Protokolün ilk nesillerinin iletişim mantığı çok basit olduğundan belirlenmesi de o derece kolay olmuştur. Napster örneğinde müdahale direk hukuk yoluyla gelmiş olsa da, ağ mühendisliğinin bu konuda izleyeceği zaten belliydi. Sunucular sadece şirkette konuşlandırıldığından ve IP'leri belirli olduğundan ağ trafiği incelenip, bu hedefle iletişimde olan IP'lerin Napster kullandığına karar verilebilirdi.

Sonraki nesillerde ise sunucu sayısının çok artması bu ilk önlem tipini işlevsiz hale getirdi. Bu aşamada daha çok "kontrol paketleri" üzerine yoğunlaşıldı. Sunucularla iletişim kuran istemcilerin sorguları ya da bu sorguların cevapları her uygulama yazılımı için belirli ve sabit portlar kullanmaktaydı. Bunun sebebi, sunucu yazılımlarının geleneksel sunucu-istemci iletişimi gibi tek porttan dinleme yapmasıydı. Her uygulama için bu portu belirledikten sonra, ağ mühendisinin belirlenen portları kullanan IP'leri tespit etmesi yeterli oluyordu. Ancak uygulama programcılarının bu belirleme şekline tepkisi çok hızlı oldu ve uygulamalarda her türlü iletişimde dinamik port kullanılmaya başlandı. Kullanılan sabit portlara örnekler Tablo 1'de verilmiştir.

Uygulama	Sabit Port
DirectConnect	411
Kazaa,Morpheous	1214
Napster-winmx	6699
Edonkey	4660-4669
Emule	4672
Bittorent	6881-6889

Tablo 1: P2P portları

Dinamik port kullanımının P2P trafiğinin belirlenmesine çıkardığı zorluk etkisini hızlıca göstermiş ve 2003 yılı sonunda çoğu ağda P2P protokolü bant genişliğinin %50'den fazlasını kullanır hale gelmiştir [6]. P2P protokolünün paylaşım amacından gelen bant genişliğini mümkün olduğunca çok kullanan yapısı ve paylaşılan dosyaların büyük çoğunluğunun telif hakkı yasaları ile korunuyor olması bu konudaki belirleme çalışmalarının en büyük motivasyon kaynaklarıdır.

Belirleme çalışmalarındaki bir sonraki adım, protokole ait kontrol ve veri paketlerinin IP başlığında yer alan ve her uygulama için "tek" olan belirli karakter dizilerinin ortaya çıkarılması olmuştur. Uygulamalar, kendine ait paketleri imzalamak için, IP başlığına bu dizileri eklemektedir. Yapılan çalışmalar sonucu ortaya çıkan imzaların bir kısmı Tablo 2'de verilmiştir [6].

Uygulama	İmza
eDonkey2000	0xe319010000
	0xc53f010000
Fasttrack	"Get /.hash"
	0x270000002980
BitTorrent	"0x13Bit"
Gnutella	"GNUT", "GIV"
	"GND"
MP2P	GO!!,MD5,SIZ0x20
DirectConnect	"$MyN","4Dir"
	"$SR"
Ares	"GET hash:"
	"Get sha1:"

Tablo 2: P2P imzaları

Belirleme yöntemi olarak bu imzaların kullanılması, ağ trafiğinde araya girerek paketlerin belirli seviyelere kadar açılıp başlıkların okunması işlemini gerektirmektedir. Çoğu ağda kullanılan firewall uygulaması bu işlem için uygun olduğundan, yeni nesil firewall'lar kapsamlarına p2p modülleri ekleyerek paketler için de bu imzaları arama özelliğini kazanmışlardır. Ayrıca yönlendiriciler üzerinde işletim sistemlerinin benzer mantıkta özellikleri barındıran sürümleri, piyasa da bulunur hale gelmiştir.

Bu yöntemler, şifreli iletişimin p2p protokolüne de adaptasyonu sonrası büyük ihtimalle kullanışsız hale geleceklerdir. Başka tür önlemlerin alınması gerekeceği aşikardır.

Sonuçta ağın takip edilmesi ve ağı sömüren bilgisayarların tespit edilmesi de önemli bir unsurdur. Lokalde yönlendirici cihazlarının netflow datalarının incelenmesi birçok bilgiyi sağlayacaktır. Bu konuda Ulakbim'in detaylı trafik istatistikleri de hattı aşırı kullananları tespit etmek için önemli bir kaynaktır.

4. TEKNİK ÇÖZÜMLER

Teknik çözümleri üç ana başlıkta toplamak mümkündür:

- Saldırı Tespit Sistemi
- QoS
- Ağ Güvenlik Duvarı/IPS Çözümleri

Bu yöntemler, günümüzde imza tabanlı tespit yöntemine dayanmaktadır. Bilindiği üzere, P2P yazılımları başlangıçta sabit port numaraları ile haberleşmekte idiler. Ancak ağ yöneticileri bu trafikleri port bazlı kesebildiklerinden, günümüzde sabit port numarası kullanan P2P yazılımı kalmamış durumdadır. Günümüz P2P uygulamaları dinamik olarak port numarası alabildikleri gibi, kullanıcılar da elle başka bir protokolün (örneğin HTTP,FTP) port numarasını atayabilmektedirler. Bu sebepten port bazlı uygulama tespiti yerine imza tabanlı uygulama tespiti zorunlu hale gelmiştir.

İmza tabanlı uygulama tespiti ağdan geçen bütün trafiğin veri (payload) kısmının kontrol edilip belirli bir örüntüye (pattern) uyup uymadığının kontrolü şeklinde yapılır. İmza tabanlı uygulama tespiti trafiğin başka bir porta yönlendirilip harici bir saldırı tespit cihazı ile yapılabileceği gibi bütün trafiğin içinden geçtiği cihazlarda (ağ güvenlik duvarı, IPS veya yönlendiricilerde) da yapılabilir. Bu çözümlerin çalıştığı sistemlerde güçlü işlemcilere gereksinim duyulacaktır.
P2P trafiğini belirleme konusunda gelinen en başarılı yöntem imza tabanlı çalışma olsa da bu konudaki çekincelerimizi belirtmekte fayda olduğunu düşünüyoruz. Bu imzalara dayalı bir yasaklama yapmak, aynı karakter serilerinin bir araya geleceği ancak p2p iletişimine dahil olmayan paketleri de engelleyebilir. Ayrıca her paketin belirli bir seviye kadar açılması, iletişime bir gecikme eklemekle birlikte akan paket sayısı çok fazla olan ağlarda, yazılım ve donanım iyi seçilmez ise firewallda tamponların dolmasına ve paketlerin düşürülerek ağ trafiğinin kesintiye uğramasına sebep olabilir. Son olarak, ağ trafiğine kesişerek bu tip bir uygulama yapmanın, kullanıcı veri gizliliği ve güvenliği açısından yaratabileceği sakıncaları

da göz ardı etmemek gerekmektedir.

4.1. Saldırı Tespit Sıstemi

Saldırı Tespit Sistemi (IDS), bir ağ veya belirli bir sunucu üzerindeki veri trafiğini takip ederek saldırıları tespit eden ve sistem yöneticisini verdikleri alarm mesajlarıyla(e-posta, çağrı cihazı ...vb) uyaran sistemlerdir. Aynı zamanda, istenirse güvenlik duvarına veya yönlendiriciye kural yazıp gerekli engellemeleri de yapabilmektedirler. Saldırı tespit sistemleri (IDS) imza tabanlı çalışmakta ve P2P trafiğini ilk iletişimi kurmaya başladığı zaman tespit etmektedir.

Ege Üniversitesi'nde kurulan sistemde Linux işletim sistemi üzerinde çalışan Snort saldırı tespit sistemi ile mesai saatlerinde P2P engellemesi yapılmaktadır. IDS olarak Snort'un tercih edilmesinin nedeni açık kaynak kodlu ve ücretsiz olması; aynı zamanda da kolaylıkla özel (custom) kuralların yazılmasına izin vermesidir.
Ege Üniversitesi'nde kullanılan sistemde, ağ omurga anahtarlama cihazında yönlendiriciye giden hattın trafiği snort'un dinlediği ethernet portuna yönlendirilmektedir. Sistem mesai saatlerinde çalışmakta ve P2P yakaladığı zaman diğer bir ethernet portu üzerinden "TCP END" paketi göndererek bağlantı (connection) kurulmasını engellemektedir. Sistem sadece hattı dinlediği için hatta bir yavaşlığa yol açmamaktadır. Süreçte yaşanan tek sorun, gece saatlerinde başlayan bağlantıların devam etmesidir ama bu ip'ler de trafik istatistikleri takip edilerek tespit edilmekte ve kapatma yaptırımları uygulanmaktadır.

Snort'un bu şekilde kullanılabilmesi için özel bir kurulum gerekmektedir ve detaylar [1] dökümanında anlatılmıştır. Snort kurallarının güncellenmesinde, hazır kuralları http://www.snort.org sitesinden almak veya Oinkmaster adlı yazılımla otomatik olarak yapmak mümkündür. Bundan sonra yapılması gereken ise haber gruplarını takip ederek p2p programlarının yapacağı değişikliklerin kural tablolarına aksettirilerek kuralların güncel kalmasını sağlamaktır.

Örneğin aşağıdaki kural, iç ağdan dışarıya yapılan bağlantılarda, içinde "User-Agent\: Ares" geçen paket paketlerin bağlantısınını sıfırlayacaktır (reset):

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg: "BLEEDING-EDGE P2P Ares traffic"; flow: established; content:"User-Agent\: Ares"; reference: url,www.aresgalaxy.org; classtype: policy-violation; sid: 2001059; rev:3; resp:rst_all;)
```

Yukarıdaki örneklerden de anlaşılacağı üzere, bu yöntem sadece TCP tabanlı çalışabilmektedir. UDP bazlı çalışan uygulamalar engelenememektedir.

4.2. QoS

P2P projesi kapsamında, İstanbul Teknik Üniversitesi'nde P2P trafiğini önlemek/kısıtlamak için Cisco yönlendirici ve üçüncü katman anahtarlama cihazlarında Quality of Service (QoS) ile Network-Based Application Recognition (NBAR) uygulaması denenmiş ve elde edilen deneyim [2] dökümanında toplanmıştır.

QoS (servis kalitesi) gecikme ve bant genişliği bakımından hassas olan uygulamalara gereken şartları sağlamak için uygulanan çözümlerdir. Servis Kalitesini sağlamak için en yaygın kullanılan metod IP paket başlığında bulunan ToS (Type of Service) kısmına öncelik vermek amacı ile numara verilmesidir. Verilecek bu numara ile, yönlendirici interface'inde pakete öncelik verilebileceği gibi, paket çöpe de atılabilir. P2P uygulamaları da bu teknik ile trafik dışı bırakılabilir.

Uygulamalara öncelik vermek amaçlı yapılan QoS temel olarak TCP veya UDP port numaralarını göz önüne alır. Portların değiştirelebileceği göz önüne alındığında, imza tabanlı uygulama tespiti zorunlu hale gelmiştir. Bu amaçla Cisco yönlendirici cihazlarına IOS 12.0(5)XE2 sürümünden sonra NBAR isimli uygulama eklenmiştir. NBAR paketlerin veri kısmını da inceleyerek uygulamanın ne olduğunu belirleyebilmektedir. NBAR Cisco'nun geliştirdiği CEF (Cisco Express Fowarding) teknolojisini kullanmaktadır. CEF yönlendiricilerin daha hızlı anahtarlama yapabilmesi için Cisco'nun geliştirdiği bir teknolojidir [3]. CEF ile yönledirici akan trafik için özel tablolar oluşturur ve aynı trafik devam ettiği sürece donanım olarak anahtarlama devam eder. CEF sayesinde NBAR trafikte pek bir gecikmeye sebep olmaz ve ayrıca yönlendiriciye de az bir işlemci yükü ekleyecektir.

Nbar ile tanımlanabilen P2P uygulamaları [3], [4] de detaylı olarak ele alınmıştır. NBAR konfigürasyonu hakkında detaylı bilgi için bkz [2]. QoS'in üzerinde çalışacağı sistemin yeterli işlemci gücüne, flash ve hafıza miktarına sahip olması, ayrıca da gereken IOS'in yüklenmiş olması gerekmektedir.

İTÜ'de NBAR ile yapılan denemelerde hepsinde olmasa da bazı P2P uygulamalarında yüksek oranda tespit yüzdeleri gözlemlenmiştir. Zaman bazlı yazılabilen erişim kural listeleri ile de mesai saatleri içersinde P2P trafiğinin yönlendiriciye fazla yük getirmeden kesilebileceği tespit edilmiştir. Ayrıca NBAR'in "protokol-discovery" özelliği sayesinde ağ kullanımındaki trafik oranlarında gerçekçi olarak saptanabilmiştir.

4.3. Ağ Güvenlik Duvarı / IPS

Ağ güvenlik duvarları imza tabanlı veya port tabanlı olarak P2P trafiğini bloklayabilmektedir. Günümüzde imza tabanlı teknikler tercih edilmektedir. Bu tür sistemlerde "ip tables" gibi açık kaynak çözümler veya donanım/yazılım tabanlı ticari çözümler kullanılabilir.

Saldırı Engelleme Sistemleri (IPS), bir ağ veya sunucu üzerindeki veri trafiğini denetleyen, saldırı olduğu tespit edilen veya istenmeyen trafiği durdurabilen sistemlerdir. IPS, IDS'in ihtiyaca göre fonksiyonları değiştirilmiş türevidir. Ağ trafiğinin üzerinden geçmesi gerekeceğinden bir miktar yavaşlamanın yaşanması muhtemeldir.

Bu çözümlerin bazılarının, saldırı tespit sistemlerinden daha başarılı olarak bağlantıları engellemeleri mümkündür ama bütün Internet erişimini bir miktar yavaşlatacaklardır. Kullanılan cihazların yeterince güçlü olması durumunda, bu yavaşlama çok az ve ihmal edilebilir bir seviyede olabilecektir.

5. SONUÇ

Bu çalışma, ULAKNET ağının daha verimli olarak kullanılması için tarafımızdan yapılan araştırmaların özetidir. Bu araştırmaların rapor halinde üniversitelerin teknik sorumlularının dikkatine sunulması hedeflenmektedir. Üniversitelerin ortak bir paydada anlaşması ve ortak kararları uygulamaya alması gerekmektedir.

Yönetmekte olduğumuz kurumsal ağın düzgün bir şekilde çalışması ve oluşabilecek hukuki sorunlara karşı hazır olunması için P2P protokolünün kontrol altında tutulması gerekmektedir. Bunun için teknik methodlar önerilmiştir.

Tarafımızdan önerilen çözümde, imza tabanlı bir tespit yöntemi kurumsal ağda uygulanmalı ve P2P protokolüne ait olduğu tespit edilen ağ trafiği belirli bir bant genişliğinde sınırlandırılmalıdır. Bu yöntem ağda kullanılan diğer iletişim protokolleri için yeterli miktarda bant genişliği sağlayacak, aynı zamanda P2P protokolünün faydalı özelliklerinin de kullanılmasına imkan verecektir. Bir başka çözüm olarak ise, mesai saatlerinde P2P trafiğinin engellenmesi önerilebilir.

Buna ek olarak, kurumsal ağımızdaki aktif bilgisayarları ve kullanıcılarını belirleyebilecek bir ağ yapısına kavuşmamız gerekmektedir. Bu sayede, P2P protokolü ya da başka bir protokol kullanılarak yapılan yasadışı hareketlerde sorumluların tespiti kolaylaşacaktır.

KAYNAKLAR

[1] Fetah V., P2P engellemek için Snort IDS kullanılması, Ege Üniversitesi Network Güvenlik Grubu

[2] Akin G., P2P Engellemek İçin QoS İle Cisco Nbar Kullanılması, İstanbul Teknik Üniversitesi Bilgi İşlem Daire Başkanlığı

[3] Network-Based Application Recognition and Distributed Network-Based Application Recognition, http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/ 121limit/121e/121e1/dtnbarad.htm

[4] Network-Based Application Recognition, http://www.cisco.com/en/US/products /ps6616/products_case_study09186a00800ad0ca.shtml

[5] Subhabrata Sen, Oliver Spatscheck, Dongmei Wnag Accurate, Acalable In-Network Identification of P2P Traffic Using application signatures

[6] Alexandre Gerber, Joseps Houle P2P, In The Cable AT&T Research Labs Research