Derin Veri Analizi: İnternet'teki Temel Gözetim Aracı

Melih Kırlıdoğ
Marmara Üniversitesi, Türkiye / North-West Üniversitesi, Güney Afrika
melihk@marmara.edu.tr

Işık Barış Fidaner
Boğaziçi Üniversitesi, Türkiye
fidaner@alternatifbilisim.org

Giriş

İnternet, üzerinden iletilen mesajlar karşısında tarafsız bir iletişim ortamı olarak tasarlanmıştır. *Net tarafsızlığı* denilen bu özellik esas olarak paketlerin yalnızca adres bölümünü okuyup içeriğini okumayan router'lar ile gerçekleşmiştir. İnternet askeri ve akademik amaçlar için ilk kurulduğu zamandan itibaren uzun bir süre net tarafsızlığı egemen olmuş, 1990larda WWW'in kuruluşuyla İnternet sıradan insanlara ve ticari dünyaya doğru eşi benzeri görülmemiş bir yayılım göstermiştir.

Bu yayılımın bir yan etkisi olarak İnternet alanında güvenlik ihlalleri sıklaşmış, bu yüzden değerli bilgileri korumayı amaçlayan çeşitli türlerde güvenlik yazılımları geliştirilmiştir. Bu bağlamda *Intrusion Detection Sistemleri* ortaya çıkmıştır. IDS sunucu ve ağlardaki saldırıları algılayıp engellemeyi amaçlar. Buna dönük olarak, sunucu veya ağdaki etkinlikleri sürekli izleyerek, ya bilindik zararlı yazılım imzalarıyla karşılaştırır ya da sistemdeki bozuklukları algılamaya çalışır. IDS, ağdan akan verilerin içeriğinin de incelenmesini içerdiği için net tarafsızlığı ilkesi, organizasyonel sınırlar içinde de olsa ihlal eder.

İnternet'in sürekli artan önemi, kısmen IDS'ten ilham alan, *Derin Veri Analizi* (Deep Packet Inspection - DPI) adında yeni bir kavramın gelişimini hazırlamıştır. Paketlerin yalnızca adres kısmını işleyen geleneksel router donanımı ve yazılımından farklı olarak, DPI sistemleri paket içeriğinin hepsini veya çoğunu inceler. 7 katmanlı OSI modeline göre bu yalnızca üstbilgi veya adreslemenin yapıldığı ilk katmanı (fiziki katman) değil, yedinciye kadarki bütün katmanların incelenmesidir. Bu yolla paketlerin bütün içerikleri analiz edilmekte ve DPI sistemi iletişim içeriğini algılayıp sınıflandırmanın yanısıra başka bir ortama kopyalayıp işlemeyi sürdürebilmektedir. Sadece 1-4 katmanlarını inceleyen, *Sığ Veri Analizi* (Shallow Packet Inspection) denilen yöntemler de vardır. DPI süreci, bir posta idaresinin elindeki mektupları yalnızca adresine iletmek yerine, hepsini açıp içlerini okumasına benzetilebilir. Bu yüzden DPI uygulamasının özel yaşam ve bilgi güvenliği açısından ciddi sonuçları vardır. Ayrıca, belirli bir organizasyonu ilgilendiren IDS'in aksine, DPI sistemleri İnternet Servis Sağlayıcılar (Internet Service Provider - ISP) tarafından uygulanmakta ve ISP'leri kullanan nüfusların tamamını olası özel yaşam ihlallerine açık hale getirmektedir.

DPI ve kullanımı

DPI'ın temel ilkesi bir kulak misafirininkine benzer: üçüncü bir taraf gönderici ve alıcıya şeffaf olacak şekilde iletişim akışına dahil olur. DPI, paketlerin "sıradışı" bir kullanımı olduğu

için izlediği ağ üzerindeki çeşitli türlerdeki iletişim akışlarına müdahale edip onları sınıflandırmasını sağlayan "hack" veya yordam parçalarından oluşur. Bu süreçte HTTP veya VoIP gibi iletişim protokollerini algılamak için genelde örüntü eşleme teknikleri kullanılır (Chen at al., 2009).

DPI bir organizasyon içinde de kullanılabilir, ulusal düzeyde de. Tek bir organizasyonun ağındaki akışları izlemek için kullanıldığında, ağ güvenliği, yük dengeleme, İnternet kullanımının kısıtlanması veya izlenmesi gibi kuruluşa ait özel ihtiyaçlara göre tasarlanmıştır. Öte yandan eğer DPI bir ISP tarafından ulusal düzeyde akışları izlemek üzere kullanılırsa, izlemenin "derinliği" de bu ölçüde değişir.

Ölçek ne olursa olsun, DPI kullanımı iki boyut içerir: ilk olarak, ağ üzerinde beklenilen iletişim düzenlerinin önceden kodlanmış yordamlar aracılığıyla otomatik olarak dayatılması, ikinci olarak ise bu yordamların elle yeniden tanımlanması, geliştirilmesi ve yeniden üretilmesi.

Temel çerçeveyi paylaşsalar da, geniş ölçekteki DPI sistemlerinin teknik zorlukları birçok düzeyde katlanarak artar:

- İzlenecek daha çok paket vardır ve daha kısa zaman aralıklarıyla gelirler.
- Bu paketler aynı anda süren daha çok sayıda iletişim akışına aittirler.
- Bu akışlar daha çeşitli iletişim protokol ve düzenlerine uygun olarak sürerler.
- Bu protokol ve düzenler zaman içinde daha çabuk çeşitlenirler. Her teknoloji kendi iletişim modelini getirdiği için teknoloji gelişiminin üstel trendini izlerler.

Bu zorluklarla baş etmek için DPI sistemleri birçok yönde geliştirilmiştir:

- Daha yüksek performans için donanım kullanımı ve koşut programlama.
- (1) İletişim akışına hat-içi/eşzamanlı/anlık müdahale veya (2) paketlerin kaydedilerek hat-dışı/eşzamansız olarak işlenmesi gibi farklı yöntemler arasında geçiş yapabilme.
- Değişken veritabanlarıyla DPI sisteminin varolan iletişim protokol ve düzenlerine dair "bilgisinin" güncellenmesi ve artırılması.

Organizasyonel DPI kullanımından daha belirgin olan ulusal düzeyde DPI kullanımının temel üç alanı vardır:

- Bunlardan ilki **ağ izlemedir**, yani bir ağın, kullanıcıların tamamı, bir kesimi veya tek tek kullanıcılar tarafından nasıl kullanıldığını anlamaktır. Bu genelde ISP'lerce eniyileme amacıyla uygulanmaktadır. Eniyileme, ISP'nin routerlarından geçen veri içeriğini bir ağ yöneticisi gibi denetleyerek "iyi" veya "akli" iletişim akışlarını "kötü" veya "yüklü" iletişim akışları karşısında ayrıcalıklandırmayı içerir.

  Örneğin ISP'ler DPI kullanarak, yüklü ağ trafiği isteyen BitTorrent dosya paylaşımı protokolünü sıklıkla kullanan aboneleri tespit edebilir, bu işlemlerden para kesebilir veya tamamen engelleyebilirler. Aynı şekilde akış içeriğinin ISP'lerce tespiti zararlı yazılım engelleme veya telif hakkı korunması gibi farklı politikaları dayatmalarına izin verir. Tekil aboneleri hedefleyen tüm bu kullanımların yanısıra DPI istatistiksel

olarak belirli bir kullanıcı kesiminin ağ kullanımını ciro ile karşılaştırarak ne kadar kar getirdiğini araştırmak için kullanılabilir.

- İkinci kullanım ISP'lerin ticari ortaklıkları ve bu alanda uzmanlaşan DPI şirketleri tarafından yapılan **hedefli reklamcılıktır** (veya Çevrimiçi Davranışsal Reklamcılık – Online Behavioral Advertising). Hedefli reklam Internet ortamında kullanıcının davranışlarını takip ederek ilgi alanlarının saptanması ve bu ilgi alanlarına göre kendisine reklam gösterilmesidir. Google ve diğer birçok kuruluş hedefli reklam uygulaması yapmaktadırlar. Ancak çoğunun yöntemlerinde DPI yoktur, "hedef"in ilgi alanları arama sözcükleri ve ziyaret ettikleri web adresleri ile belirlenir. Hedefli reklam için DPI kullanıldığında ise daha "derin" ve daha anlamlı verilerle daha isabetli hedefleme yapılabilir. Bu genelde abonenin bilgisayarına cookie'ler bırakarak yapılır. Bütün abonelere tekil kimlik numaraları verilir ve ilgi alanlarını belirlemek için bütün etkinlikleri kaydedilir. Kullanıcılar teorik olarak bilgilerinin toplanmasını engelleyebilir veya o hizmeti kullanmayı bırakabilir, ama bazı daha karmaşık sistemler cookie'ler silindiğinde dahi kullanıcı hakkında bilgi toplamayı sürdürmektedirler.

- Üçüncü kullanım ise devletlerce yasal veya yasadışı gözetim ve sansürdür. Bunlar, çocuk pornografisi gibi genel kabul görmüş suçların engellenmesinden, ülkedeki muhalif hareketlerin baskılanması gibi baskıcı eylemlere kadar farklı biçimler alabilir. Genelde amaç ikincisidir ve ilki DPI kurulumunu gerekçelendirmek için kullanılır. Devletler DPI gözetimi için ISPlerin rıza ve işbirliğine ihtiyaç duyarlar. Bu çoğunlukla fazla zorluk yaratmaz, çünkü ISP'ler çalışabilmek için devlet iznine tabidirler. Sonuç olarak DPI sistemi sınırsızca gözetim için kullanılır ve bu kendini tetikleyen bir merak sonucunda, er ya da geç, ağ kullanıcısının özel yaşamı ihlal edilir.

Birçok devlet, bütün yurttaşlarının İnternet iletişimini kaydetmek istemesine rağmen toplumsal ve teknik engellerle karşılaşır. Teknik zorluklar temelde akan verinin muazzam büyüklüğünden gelir. Veriler kaydedilse dahi, detaylı olarak analiz edilmesi yine zorluklar içerir. "Elektrik süpürgesi" yaklaşımı denilen, bir kanaldan akan bütün iletişim sinyallerinin analiz edilmesi, DPI için gerçeklenebilir değildir. Yine de ISP'lerde yer alan özel DPI "kutuları" yoluyla tekil abonelerin teknik takibe alınması her zaman mümkündür.

Bazı ülkelerde gözetim amacıyla DPI kullanılması

Amerika Birleşik Devletleri:
DPI ABD'de bir denetim ve gözetim aracı olarak yoğunlukla kullanılmaktadır. James Bamford *The Shadow Factory* isimli kitabında bu kullanımı ayrıntılı bir şekilde anlatmaktadır. Buna göre bu ülkedeki Internet pazarının büyük bir kısmını kontrol eden AT&T ve Verizon şirketleri DPI uygulamalarını bu alanda uzmanlaşmış iki şirket vasıtasıyla yapmaktadırlar. AT&T'nin iş ortağı Narus, Verizon'un iş ortağı ise Verint isimli şirketlerdir. Bu şirketler asıl olarak Internet trafiğinin geçtiği tesislerde kendilerine ayrılan ve başkalarının erişimi yasaklanmış özel odalarda faaliyet göstermektedirler. Internet trafiğinin bir kopyası bu odalardaki Narus ve Verint cihazlarından geçerek NSA (National Security Agency) bilgisayarlarına gitmektedir.

Bamford'a göre hem Narus hem de Verint şirketleri İsrail ve bu ülkenin casusluk teşkilatı Mossad ile içiçedir. Verint eski bir Mossad elemanı olan Jacob Alexander tarafından

kurulmuş olup bu kişi halen aralarında hırsızlık, sahtekarlık, yalancılık, rüşvet ve kara para aklama gibi otuzdan fazla suç nedeniyle FBI tarafından aranmaktadır. Narus ise 1997'de beş İsrail vatandaşı tarafından kurulmuştur. Bamford bu beş kişinin erişilebilen hayat hikayelerindeki boşlukların İsrail askeri kuruluşlarıyla ilgili olduğunu ima etmektedir. Narus 2010 senesinde ABD havacılık şirketi Boeing tarafından satın alınmıştır.

Bamford bir ABD vatandaşı olarak bu ülkedeki Internet trafiğinin tamamına yakınının Verint ve Narus şirketlerinin donanımları üzerinden geçtiğinden yakınmaktadır. Kendisinin bir diğer yakınma konusu bu cihazlardan geçen trafiğin uzaktan kolayca denetlenebilmesidir. Bu noktada ABD vatandaşı olmayanların da kaygı duymaları gerekmektedir. Çünkü Internet trafiğinin önemli bir kısmının ABD üzerinden geçmektedir. Örneğin, Çin'den Japonya'ya gönderilen bir mesajın ABD üzerinden geçmesi (ve geçerken bir kopyasını da bu cihazlara bırakması) büyük bir olasılıktır. İsrail casusluk teşkilatlarının muazzam boyutlardaki mesajları veri madenciliği yoluyla analiz etme kapasitesi muhtemelen sınırlı olmakla birlikte hedeflenmiş mesajların bu ülkenin gözetimine açık olması tüm dünyada kaygı uyandırmaktadır.*

İngiltere:
İngiltere AB ülkeleri arasında kendi vatandaşlarını dinlemek konusunda kötü bir üne sahiptir. Bu ülkenin elektronik casusluk teşkilatı GCHQ (Government Communication Headquarters) Internet üzerinden iletişimin gitgide daha fazla önem kazanması üzerine 2008 yılında Interception Modernisation Programme (IMP) adlı bir proje başlattı. İki milyar sterlin bütçeli IMP asıl olarak Internet ağırlıklı olmakla birlikte telefon dinlemelerini de kapsamaktaydı. Proje kapsamında ülkedeki Internet Servis Sağlayıcı (ISS) şirketlerinin tüm tesislerine DPI donanımı yerleştirilmesi öngörülmekteydi. Proje açıklandıktan sonra tüm ülkede büyük bir muhalefet dalgasıyla karşılandı. Diğerlerinin yanında saygın London School of Economics bir rapor hazırlayarak projenin neden uygulanmaması gerektiğini inceledi (bkz. http://www2.lse.ac.uk/management/documents/IMP-briefing.pdf). Yoğun muhalefet nedeniyle İngiltere hükümeti projeyi geri çektiyse de kısa bir süre sonra yaklaşık aynı içerikli "Communications Capabilities Development Programme" adlı başka bir proje başlattı.

Türkiye:
Türkiye'de tüm yönleriyle bilinen tek DPI uygulaması 2012 yılında faaliyete başlayan TTNET-Phorm ortaklığı kapsamında "davranışsal reklamcılık" girişimidir. Phorm, kişisel mahremiyeti ayaklar altına alan sistemi nedeniyle ABD, İngiltere ve Güney Kore'den sonra Romanya'da da faaliyetleri yasaklanan ve gittiği her ülkede şiddetle muhalefet gören şaibeli bir organizasyondur. Türkiye'de de kendisine karşı güçlü bir muhalefet sürdürülmektedir (bkz. Enphormasyon.org). Bu muhalefet sonucunda BTK TTNET-Phorm işbirliği hakkında "kullanıcıları yanılttığı" ve "talep etmeyenleri de kendi sistemleri içine aldığı" gerekçeleriyle soruşturma açmış ve sistem "Gezinti" isimli sistem içindeki tüm kullanıcıların sistem dışına çıkarılmasına karar vermiştir. TTNET-Phorm işbirliğinin Internet kullanıcıları açısından en

*ABD'nin kendi vatandaşlarının ve tüm dünyanın Internet trafiğini İsrail kökenli şirketler vasıtasıyla dinlemesi İsrail'in bu ülkedeki yoğun etkisinin bir tezahürüdür. Bu etki eski bir CIA yöneticisi tarafından yazılan kitapta özlü bir şekilde şöyle anlatılmaktadır: "Tarihte 6 milyonluk bir ülkenin 270 milyonluk başka bir ülkedeki politika ve güvenlik söylemini denetlediği başka bir örnek yoktur." Bu denetim öylesine yoğundur ki, kitabın yazarı muhtemelen gelecek tepkilerden sakınmak için yazdığı kitapta adını açıklayamaktadır. Sonradan adının Michael Scheuer olduğu ortaya çıkan yazar "The Imperial Hubris" isimli kitabını ancak "Anonymous" rümuzuyla bastırabilmiştir.

sakıncalı yönü kişisel mahremiyetini korumak isteyen kullanıcılara kaçış imkanı bırakmamasıdır. Çünkü Türkiye'de Internet omurgası TTNET tarafından kontrol edilmektedir.

Belli ölçülerde şeffaflığın olduğu ve DPI konusunda serbest tartışmaların yapılabildiği Batı ülkelerinin aksine Türkiye'deki DPI vasıtasıyla gözetim uygulamaları bir sis perdesinin ardındadır. Ülkede halen fazla etkin olmayan bir DPI sisteminin olduğu ve daha "iyisinin" geliştirilmesi sürecinin halen devam ettiği yolunda belirtiler mevcuttur.

Sonuç

Internet ortamında DPI kullanımının çeşitli türleri vardır. Bunlardan bazıları kişisel mahremiyet için zararsız, bazıları ise son derece zararlı niteliktedir. Bu ikisinin arasında belli trafiğin hızını azaltmak veya trafiğin içeriğine göre ücret belirlemek gibi gri alanlar bulunmaktadır. Ancak gerek davranışsal reklamcılık, gerekse de devlet gözetimi uygulamaları kapsamında kişisel mahremiyet açısından DPI kabul edilemez niteliktedir.

Türkiye Cumhuriyeti Anayasasının 20. maddesinde "özel hayatın ve aile hayatının gizliliğine dokunulamaz" ve 22. maddesinde "haberleşmenin gizliliği esastır" denmesine rağmen Türkiye'de yaşayan herkes telefonunun dinlendiğinden veya ilerde kendi aleyhine kullanılmak üzere kaydedildiğinden emindir. Öyle ki, hükümet üyeleri bile "dinlemelerin rezil bir noktaya geldiğini" söyleyebilmektedirler (bkz. http://www.memurlar.net/haber/319698/). Internet üzerinden gözetim telefon dinlemeye kıyasla çok daha zor olmasına rağmen imkansız değildir. Eğer karşı çıkılmazsa DPI teknolojisi sayesinde ilerde Türkiye'deki Internet iletişiminin telefon iletişiminin şimdiki haline döneceğine inanmak için yeterli neden mevcuttur.

Kaynaklar

Anonymous. (2004). *The Imperial Hubris: Why the West is Losing the War on Terror.* Washington D.C.: Brassey's Inc.

Bamford, J. (2008). *The Shadow Factory.* New York: Anchor Books.

Bellman, S, Johnson, E. J., Kobrin, S. J. & Lohse, G. L. (2004). "International Differences in Information Privacy Concerns: A Global Survey of Consumers ," *The Information Society*, 20(5), pp. 313–324.

Bloomberg (2011). http://www.bloomberg.com/news/2011-12-22/spies-fail-to-escape-spyware-in-5-billion-bazaar-for-cyber-arms.html

Chen, Z., Zhang, Y., Chen, Z. & Delis, A. (2009). "A Digest and Pattern Matching-Based Intrusion Detection Engine," *The Computer Journal*, 52(6), pp. 699–723.

Conti, J.P. (2011). "Is Seeing Deceiving?" *Engineering & Technology*, April, pp.70-71.

Dutta, S., Dutton, W.H. and Law, G. (2011) "The New Internet World. A Global Perspective on Freedom of Expression, Privacy, Trust and Security Online." Contribution to: The Global Information Technology Report 2010-2011. Transformations 2.0. World Economic Forum, April 2011.Dutton, WH., Dutta, S. and Law, G.

Elaman (2012). www.elaman.de Accessed 17 August 2012.

Fuchs, C. (2012). “Implications of Deep Packet Inspection (DPI) Internet Surveillance for Society,” Department of Informatics and Media, Uppsala University.

Goodman, S. & Harris, A. (2010). “The Coming African Tsunami of Information Insecurity.” *Communications of the ACM*, 53(12), pp.24-27.

Hofstede, G. (2001). *Culture’s Consequences*. Second Ed. Thousand Oaks, CA: Sage.

Mason, R.O. (nodate). “A Tapestry of Privacy, A Meta-Discussion,” http://home.aisnet.org/displaycommon.cfm?an=1&subarticlenbr=553

Parker, P. M. (2009). “The 2009-2014 Outlook for Deep Packet Inspection (DPI) Test Equipment in Africa & the Middle East ,” www.icongrouponline.com

TI. (2012). https://www.privacyinternational.org/projects/big-brother-inc Accessed 18 August 2012.

WSJ. (2011). http://online.wsj.com/article/SB10001424053111904199404576538721260166388.html Accessed 17 August 2012.