

Eşler Arası Ağlarda Teşvik Modelleri

Serkan Çakmak, Ahmet Burak Can

Özet—Eşler arası ağlar, kaynak paylaşımı, yönlendirme, ve kaynak arama gibi görevlerde eşlerin katkı sağlaması ilkesine göre çalışır. Eğer eşlerin bir kesimi, sisteme bu görevlerde katkı sağlamazsa, sistem verimliliği ve etkinliği önemli zarar görür. Bu bildiri, eşler arası ağlarda eşleri teşvik ederek sisteme katkıda bulunmalarını sağlamak üzere tanımlanmış olan teşvik yaklaşımları üzerine bir literatür taraması sunmaktadır. Teşvik modellerinin neden ortaya çıktığı, bu amaçla hangi yöntemlerin uygulandığı ve bazı yaygın eşler arası uygulamalarda kullanılan teşvik modelleri anlatılacaktır.

Anahtar Kelimeler—Eşler arası ağlar, teşvik modelleri, oyun teorisi, karşılıklılık, mikro para modelleri

Incentive Models in Peer-to-Peer Networks

Abstract— Peer-To-Peer networks work relying on involvement of peers on tasks like resource sharing, routing, and querying of resources. If some peers do not contribute to the system, efficiency and effectiveness of the system is damaged. This paper presents a literature review about incentive approaches in peer-to-peer networks used to encourage peers to contribute to the system. Why incentive models are appeared, approaches applied for this goal, and some incentive models used by common peer-to-peer applications will be explained.

Index Terms—Peer-to-peer networks, incentive models, game theory, reciprocity, micro money models

I. GİRİŞ

Bilgisayar ağlarının gelişimine baktığımızda, son senelerde eşler arası ağlar (peer-to-peer- P2P), istemci-sunucu mimarisi yanında alternatif bir ağ modeli olarak ortaya çıkmıştır. İstemci-sunucu mimarisinde bir tane veya birkaç sunucu bulunmakta ve diğer bütün istemciler bu sunuculardan indirme işlemini gerçekleştirmektedirler. Bu durumda merkezi bir yönetim ve hataya duyarlı tek bir nokta (single point of failure) olduğu net bir biçimde görülmektedir. Ayrıca, her istemcinin indirme hızı, sunucunun paylaşılan yüklemeye hızı ile sınırlı kalmaktadır. Ancak P2P ağlarda ortada bir istemci ve sunucu yoktur. Her eş aynı anda istemci ve sunucu olabilir. Bir eş başkalarına hizmet sağlarken sunucu görevi görebilirken, başkalarından hizmet elde etmek için de istemci görevini üstlenir. Bu ağlardaki eşlerin, hem istemci, hem de sunucu olarak görev yapabilmesi tamamen dağıtık ağ topolojileri tanımlamaya imkan tanımaktadır. P2P sistemler, dağıtık olmaları nedeni ile dosya dağıtım sistemleri için istemci-sunucu mimarisine ciddi bir alternatif olmuşlardır.

Bu metin 15 Temmuz 2013 tarihinde gönderilmiştir.
Serkan Çakmak, Hacettepe Üniversitesi Bilgisayar Mühendisliği Bölümü'nde Yüksek Lisans yapmaktadır. (e-mail: serkancakmak89@gmail.com).

Ahmet Burak Can, Hacettepe Üniversitesi, Bilgisayar Mühendisliği Bölümü'nde görev yapmaktadır. (e-mail: abc@hacettepe.edu.tr).

P2P ağlarda, eşlerin ağ üzerinde yürütülen dağıtık işlemlerde görev alması ve sisteme kaynak sağlaması, ağın devamı açısından çok önemlidir. Bazı durumlarda eşler, ağa hiç katkı sağlamadan sistem kaynaklarını kullanmaya çalışmakta veya ağın kaynakları kullandıktan sonra ağa katkı sağlamayı bırakmaktadır [1]. Bu durum, ağın etkinliğini ciddi ölçüde etkilemekte ve bazı eşlere fazla yük binmesine sebep olabilmektedir. Bu nedenle, ağ üzerindeki bütün eşleri sistem katkı sağlamaya motive etmek ve bazen de zorlamak üzere teşvik (*incentive*) modelleri önerilmiştir. Teşvik modelleri, P2P ağlarda çeşitli yöntemler uygulayarak kaynak paylaşımını artırmayı amaçlayan modellerdir. P2P ağlarda eşleri daha fazla sisteme katkı sağlamaya teşvik etmek ve sisteme herhangi bir fayda sağlamadan sistemden yararlanan kullanıcıları engellemek teşvik modellerinin en önemli görevidir.

Bu bildiri, teşvik modelleri hakkında yapılmış çalışmalar incelenecektir. Kesim II'de teşvik modelleri üzerine yapılabilecek saldırılar irdelenecektir. Kesim III'te teşvik modelleri ve iktisat teorileri arasındaki ilişki açıklanacaktır. Kesim IV'te teşvik modellerinde kullanılan bazı temel yaklaşımlar aktarılacaktır. Kesim V'te sonuçlar ve gelecekte yapılabilecek çalışmalar özetlenecektir.

II. EŞLER ARASI PAYLAŞIM PROBLEMLERİ

P2P sistemlerin gücü, eşlerin gönüllü paylaşımından gelmektedir. P2P sistemlerinde merkezi bir otoritenin olmaması ve gücünün gönüllü paylaşımından gelmesi teşvik modellerini kaçınılmaz olarak ortaya çıkarmıştır. Çünkü istemci-sunucu mimarisinde indirme için sunucunun kurallarına uymak zorunda olan kullanıcılar, eşler arası ağlarda yöneticinin olmaması nedeniyle rasyonel davranışlar göstererek kendi kişisel karlarını en fazla yapmaya çalışırlar. Bu rasyonel davranışa sahip kullanıcılar birçok P2P uygulamanın sorunu olmuşlardır [1]. Örneğin Gnutella ve Napster üzerinde yapılan araştırmalar göstermiştir ki, bu uygulamaları kullanan kullanıcıların %50'sinin oturum süreleri 1 saatten azdır ve çoğunluğu paylaşım yapmamaktadır [2]. Kullanıcıların kendi karlarını artırma isteğinden dolayı ortaya çıkan problemler arasında en yaygın olanları, bedavacılık (*free riding*), geçmiş silme (*white washing*) ve çoklu kimlik tanımlama (*sybil attack*) problemleridir. Şimdi bu problemleri inceleyelim.

Bedavacılık (Free Riding)

Bedavacılar sisteme hiçbir katkı yapmadan sistemden yararlanan kullanıcılara denir [1,5]. Bu davranışın temel nedeni, kullanıcıların (eşlerin) kendi karlarını artırırken, sisteme herhangi bir katkı (işlemci zamanı, disk alanı, vb.) vermeden elde etmek istedikleri kaynaklara ulaşmaya çalışmalarıdır. Bu davranış biçimi, aslında insan doğasından gelen bir davranıştır. Bir kullanıcı bir şeyi bedava elde edebiliyorsa neden para/kaynak versin ki? Bu noktada,

kullanıcıları para/katkı vermeye teşvik edecek veya hatta bazen zorlayacak bir sistem olmalıdır.

Geçmiş Silme (White Washing)

Bedavacılığı önlemeye yönelik bir yöntem kullanan sistemlerde, bazen bedavacı olan kullanıcılar (eşler) sürekli olarak sistemden ayrılıp tekrar sisteme katılırlar. Böylece geçmişlerini silerek bedavacılık cezalarından kurtulmaya çalışırlar [5,24]. Özellikle itibara dayalı güven modelleri (reputation-based trust models) [25,26] bu ataklara duyarlıdır. Bu atağın ortaya çıkma nedeni, sistemdeki kimlik alma maliyetinin az olması veya olmaması ve kullanıcıların anonim olarak sisteme katılabilmeleridir. Kullanıcıların sürekli olarak kimlik değiştirip sahte kimlikle sisteme katılabilmesi çeşitli yöntemler ve cezalarla engellenmeli veya en azından zorlaştırılmalıdır.

Çoklu Kimlik Tanımlama (Sybil Attack)

Sybil saldırısında [3], saldırıyı yapan kullanıcı (eş) büyük miktarda sahte eş ve kimlikler oluşturarak sistemdeki teşvik modelini kandırmaya çalışır. Oluşturduğu sahte kimlikteki kullanıcılara sürekli olarak kaynak sağladığını iddia ederek, teşvik modelini kandırmaya ve sistemdeki diğer eşlerin kaynaklarından daha çok yararlanmaya çalışır. Sistemde güvenilir otorite olarak görev yapan bir merkez olmadığı sürece, bu atağın her zaman olma olasılığı vardır.

III. TEŞVİK MODELLERİ VE İKTİSAT İLİŞKİSİ

P2P sistemlerde teşvik modelleri ile iktisat alanı arasında ilk başta ilişki kurmak zor görünebilir, ancak P2P teşvik modellerindeki problemler, genel kullanıcı davranışları, sistemin ve kullanıcıların kar maksimize etme davranışları, iktisattaki bazı konularla oldukça paralellik göstermektedir. Şimdi sırasıyla iktisat alanından ortak malların trajedisi, oyun teorisi, ve mahkûmlar çıkmazı konularını inceleyeceğiz.

A. Ortak Malların Trajedisi Kuramı

Ortak Malların Trajedisi Kuramı [19], isminden de anlaşılacağı gibi iktisatta kamu malları gibi ortak malların yaşadığı trajediyi anlatmaktadır. Şöyle ki, kamusal mallar herkes tarafından kullanılabilir serbest, herkese yarar sağlayan, buna karşılık herhangi bir gideri olmayan mallardır. Yani bir kamu malı kullanımı sonucu yarar sağlarken, herhangi bir ücret verilmez. Bu gibi durumlarda kişiler başkalarından bağımsız olarak sadece kendilerini düşünerek, rasyonel davranışlarda bulunarak kendi karlarını maksimize ederler. Ancak böyle bir durumda, kamusal mal gereğinden çok daha hızlı sürede yaşam evresini tamamlayabilir ve tükenir. Bu duruma, kamusal malların trajedisi denir. Kamusal malların sahipliği tek bir kişi değil birçok kişiye aittir. Bu durum aslında kamusal malları sahipsiz yapmakta ve çok daha hızlı yıpranmalarına, tükenmelerine yol açmaktadır. Örneğin bir kamu alanındaki park ile bu park ile aynı yerdeki özel bir bankayı ele alalım. Her ikisinin de içinde kişilerin oturması için banklar olduğunu düşünelim. Her iki oturma bankasının da aynı kişiler tarafından kullanıldığı varsayılabilir bile ufak bir tahmin ile park içindeki bankın çok daha kısa sürede işlevini yitireceği ve eskiyeceğini tahmin etmek mümkündür.

Ortak malların trajedisi kuramı, ek olarak kamusal mallardan yararlanma ücreti konusuna da değinir. Ortak malların kullanım ücretleri herkes için sıfırdır. Bu durumda ortaya çıkan sonuç, herkes herhangi bir ücret ödemediği kamusal mallardan sınırsız fayda sağlayabilmektedir. Bu durumda kamuya katkı sağlayan bir insan ile sağlamayan bir insan ayrımı yoktur. Örneğin vergi veren ve vermeyen 2 kişiyi düşünecek olursak, bu iki kişinin de sokağındaki lamba yanmaktadır. Bu durumda vergi veren ve vermeyen kişileri nasıl ayırt edip insanları vergi vermeye teşvik edebiliriz.

Yukarıda anlattığımız ortak malların trajedisi kuramı ile ilgili problemler, P2P teşvik modellerinin karşılaştığı problemler ile benzerlikler göstermektedir. P2P sistemlerde paylaşım yapan kullanıcı ile paylaşım yapmayan kullanıcının ayırt edilmesi ve ortak sistem kaynakları kullanılırken eşlerin paylaşım yapmaya teşvik edilmesi gerekmektedir.

B. Oyun Teorisi ve Nash Dengesi

Bazı problemlerde, değişkenlerin tümü kontrolümüz altında olmayıp iki ya da daha fazla tarafça kontrol edilebilir. Yani değişkenlerin bir kısmı bizim, başka bir kısmı da başkalarının kontrolü altında olabilir. Bu durumda sorunun çözümü için şu kural uygulanır:

- Kazancı maksimum yapmak
- Eğer kazanma şansı yoksa kaybı minimum yapmak

Oyun teorisinde amaç karar verme stratejisi geliştirmektir. Modern Oyun Teorisi ilk olarak John von Neumann tarafından ortaya atılmıştır [20,21]. Oyun teorisinde genel amaç karşındaki kişinin yapacağı tercihleri de göz önünde bulundurarak kendin için en yararlı veya en az zararlı tercih için bir strateji belirlemektir. John von Neumann tarafından ortaya atılan iki kişilik sıfır toplamlı oyunda, oyun sonunda oyuncuların birinin kaybı diğerinin kazancına eşittir.

İkiden fazla sayıda oyuncunun yer aldığı oyunlarda, denge durumunu modellemeyi amaçlayan Nash dengesi yaklaşımı, ilk olarak olarak Steve Nash tarafından ortaya atılmıştır [22]. Bu modele göre, oyuncuların birbirlerinden bağımsız kararlar verdiği bir oyunda (non-cooperative game), oyuncular mevcut stratejilerini değiştirerek herhangi bir kazanç sağlayamıyor ise, bu oyuncular birbirleri ile Nash dengesindedir. Klasik Nash dengesi, diğer eşlerin hangi stratejiyi uygulayacağına dair sonsuz spekülasyon ve karşı spekülasyon döngüsünden çıkış yolu gösterir. Bir eş, denge stratejilerini değiştirirse bile, hiçbir eşin faydasını artıramadığı yerel optimum strateji kümesi böylece elde edilir.

P2P ağlarda da, kullanıcılar arası etkileşimler çok kullanıcı bir oyun olarak düşünülebilmektedir. Bir teşvik modeli ile kullanıcılar bazı davranış örüntülerine yönlendirilerek bu oyunda denge sağlanmaya çalışılmaktadır. Böyle bir denge durumunda, istenen davranıştan farklı bir davranış sergileyen (örneğin kaynak paylaşmayan) eşlerin oyun genelinde zarar etmesi sağlanmaya çalışılmaktadır.

C. Mahkûmlar Çıkmazı (Prisoner's Dilemma)

Mahkûmlar çıkmazı [23], iki bireyin karlarını maksimize etmek istemeleri durumunda, bireylerin kişisel karlarını maksimize etmek için seçtikleri stratejinin her zaman en iyi karı sağlamadığını göstermek için geliştirilmiş bir oyundur. Mahkûmlar çıkmazına göre iki tutuklu ayrı ayrı odalarda

sorgulanır. Her bir tutuklunun iki seçeneği vardır. İtiraf etmek, ve sessiz kalmak. Eğer iki tutuklu da sessiz kalırsa; iki tutuklu da birer yıl ceza alacaktır. Eğer bir tutuklu itiraf eder, diğer tutuklu sessiz kalırsa; itiraf eden serbest kalırken, diğer tutuklu on yıl ceza alacaktır. Eğer iki tutuklu da itiraf ederse; iki taraf da beşer yıl ceza alacaktır. Buna göre bireysel kar maksimizasyonu düşüldüğünde, iki tutuklu da en az cezayı almak için itiraf edecektir ve iki tutuklu da zarar görecektir. Aksine iki tutuklu da sessiz kalsa, en az ceza alınabilirdi.

P2P ağlardaki problemler kapsamında düşünüldüğünde, Oyun Teorisi, Nash Dengesi ve Mahkumlar Çıkmazı problemleri, teşvik modellerinde eşlerin paylaşım yapmıyacaklarına, katkı sağlayıp sağlamayacaklarına karar vermede kullanılabilir.

IV. TEŞVİK MODELLERİNDE TEMEL YAKLAŞIMLAR

Teşvik modelleri, yukarıda bahsettiğimiz problemlerle baş etmek ve kullanıcıları sisteme katkı sağlamaya daha fazla teşvik etmek için geliştirilmiş modellerdir. Modeller için çeşitli yaklaşımlar mevcuttur. Bu bölümde, teşvik modelleri üzerine yapılan bazı çalışmalar incelenecektir. Yaygın olarak kullanılan bazı P2P uygulamalar üzerindeki teşvik modellerine de değinilecektir.

A. Mütakabiliyet (Reciprocity) Tabanlı Yaklaşımlar

Mütakabiliyeti esas alan yaklaşımlarda, eşler diğer eşlerin geçmişi hakkında bilgi tutarlar ve bu bilgiyi paylaşım için karar vermede kullanırlar. Geçmişte bir kullanıcının sisteme sağladığı katkı bilgisi saklanarak daha sonraki hizmet alımında kendisine yarar sağlar. Bu yaklaşımlar, doğrudan ve dolaylı mütakabiliyet tabanlı olmak üzere ikiye ayrılır. Doğrudan mütakabiliyeti esas alan yaklaşımlarda, X, Y ile hangi seviyede iş birliği yapacağını, geçmişte Y'den aldığı servise göre karar verir. Yani bir eş karar aşamasında sadece kendi tuttuğu geçmişe güvenir. Doğrudan mütakabiliyet, genelde uzun süren etkileşimler içeren uygulamalar için daha uygundur. Örneğin, Bittorrent [8] uygulaması bu modeli kullanır. Deneysel ve analitik çalışmalara göre bu yaklaşım, sistemdeki işbirliğini artırdığını gösterse de, free rider problemini tam olarak çözemez [6].

Dolaylı mütakabiliyet yaklaşımında, X eşi Y eşi ile hangi seviyede iş birliği yapacağını, kendisi ve diğer eşlerin de geçmişte Y'den aldığı servise (Y'nin geçmişine) göre karar verir. Yani bir eş karar aşamasında sadece kendi tuttuğu geçmişe değil başka eşlerin tuttuğu geçmişe de güvenir. Genelde bu yaklaşım, itibara dayalı güven modelleri (reputation-based trust models) [25, 26] ile birlikte kullanılır ve doğrudan mütakabiliyet yaklaşımına göre, bedavacılık problemi için genelde daha gerçekçi sonuçlar verir. Fakat 3. parti gözleme güvenmek zorunda olduğundan geçmiş temizleme ve çoklu kimlik tanımlama saldırılarına karşı duyarlıdır.

Mütakabiliyet tabanlı bazı yaklaşımları şöyle özetleyebiliriz.

Kalıtıl Cömertlik (Inherent Generosity) [4]

James Andreoni [4] tarafından geliştirilen modelde, kullanıcı cömertliği de işin içine katılarak bedavacılık ve geçmişi silme sorunları ile başa çıkılması amaçlanmıştır. Bu modelde popülasyon dağılımına göre bedavacılık oranı

bulunması amaçlanmıştır. Bu modele göre, cömertlik/popülasyon oranı, belli bir eşik değerinin altında ise, sistemin etkin bir şekilde çalışmadığı; üstünde ise sistemin sürdürülebilir olduğunu söylenir. Benzer şekilde, [5]'in yazarları da bu yaklaşımın benzerini kullanan bir model geliştirmişlerdir.

BitTorrent [8]

BitTorrent [8] eşlerin, diğer eşlerden dosya indirebildiği dağıtık dosya paylaşım ve indirme sistemidir. Temel fikri dosyayı parçalara ayırır ve her bir parçayı farklı eşlerden indirebilir. Böylece eşler, işbirliği yaparak eksik parçaları tamamlamaya çalışırlar. Bu yöntem, hataya duyarlı tek bir notayı (*single point of failure*) ve tek bir sunucu üzerinden dosya indirmede karşılaşılan kısıtları ortadan kaldırırken, eşleri işbirliğine zorlar. Yani sistem tasarımcıları, eşler için bir teşvik modeli sağlamışlardır. BitTorrent bugün için çok yaygındır ve bu protokol üzerinde bir çok araştırma yapılmıştır. Bunun nedenleri şöyle sıralanabilir: Sistemin kullanıcıların kendi karlarını maksime edeceği düşünülerek tasarlanmış olması, sistem tasarımında bir teşvik modeli olması, sistemin analitik ve ekonomik deneyler için uygun olması ve çok yaygın kullanılmasıdır [10, 11].

BitTorrent'teki teşvik mekanizması tit-for-tat stratejisine veya mahkumlar çıkmazı modeline dayanan yüklemle ile orantılı bir indirme mekanizmasıdır. BitTorrent'te takipçiler (*tracker*) bir dosyaya tamamen veya kısmen sahip olan eşlerin listesini tutar. Dosyanın tamamına veya bir kısmına sahip her eş, takipçi tarafından takip edilir. Yeni bir eş sisteme katıldığında takipçi ile iletişim kurup, dosyayı indirebileceği eşlerin listesini takipçiden ister. Bu eşler de, yeni katılan eşle iki taraflı TCP bağlantıları kurarlar. Bu bağlantılar yardımıyla küçük bir eş altkütmesi seçilmiş olarak işaretlenir. Dosyanın tamamına veya bir kısmına sahip eşler, daha iyi işbirliği sağlayan eşleri bulmak için belli aralıklarla iyimser seçme stratejisini kullanırlar. Eşler, belli aralıklarla, sağladıkları yüklemle hızına göre, işbirliği yapacağı k tane eşi seçer. Böylece yüksek yüklemle hızı sağlayan eşler, daha çok seçildikleri için, daha yüksek indirme hızları ile dosya indirebilirler. Bu özelliklerine rağmen, Bittorrent geçmiş temizleme ve çoklu kimlik tanımlama saldırılarına karşı savunmasızdır.

BitTyrant [9]

Bazı durumlarda BitTorrent'in teşvik modeli alt edilebilir [9]. Tit-for-tat stratejisi, kaynak paylaşımı ile kaynak indirimini dengelese ve zamanla evrensel dengeye ulaşan bir strateji olsa dahi, pratikte yüksek kapasitedeki (bant genişliği yüksek) kullanıcılar, indirme işlemini daha erken bitirdikleri için kaynak paylaşımını da erken sonlandırma eğilimindedirler. Bu durum, tit-for-tat stratejisinin istenilen şekilde çalışmasını engeller ve yüksek kapasiteli kullanıcıların sistemi sömürmesine yol açar. BitTyrant uygulamasının ana fikri, BitTorrent'teki yüklemle hızından bağımsız olarak yapılan statik yaklaşımın tersine, her eş bir tit-for-tat oturumunda belli sayıda veri gönderdiği eşleri dinamik olarak seçer.

BitTyrant sisteminde d , eşin sisteme sağladığı katkı ve u , eşin kazanması gereken mütakabiliyet oranı olmak üzere, d/u oranı dikkate alınarak en yüksek orana sahip eşler seçilir. Her bir döngüde eğer bir eş sisteme katkıda bulunmamış ise onun u değeri artırılırken, bir başka eşe veri yollamış ise onun u değeri azaltılır. Yapılan deneylerde BitTyrant'ın

BitTorrent e göre 3 kat daha hızlı indirme sağladığı gözlenmiştir [9]. BitTyrant'ın bu performansı şöyle açıklanabilir: a)BitTyrant uzun süreli sürekli performans sağlar, b)yüksek kapasiteli eşler için azalan marjinal fayda prensibini içerir c)düşük kapasitedeki eşlere sistemden görece fazla fayda sağlar. Fakat BitTyrant'ın artan performansı bize bir maliyet ile döner. Yeni kullanıcıların uzun ön yükleme süreleriyle karşılaşmaları buna örnek verilebilir. Ayrıca BitTyrant, BitTorrent gibi geçmiş temizleme ve çoklu kimlik tanımlama saldırılarına karşı dirençsizdir.

Credence [7]

Credence [7] içerik kirliliğini engellemek için tasarlanmış bir dağıtık itibar sistemidir. Credence sistemi ile kullanıcı, dosyanın veya online içeriğin gerçekten iddia edilen dosya/içerik olup olmadığına karar verebilir. Kullanıcılar sistem içeriklerini oylarlar ve sistem benzer oyları ağırlıklandırır. Bir benzerlik ölçütüne (*similarity measure*) göre, doğru oyları yüksek ağırlık vererek, sahte oyları ise düşük ağırlık vererek değerlendirir. Böylece kullanıcılara doğru oy vermeleri için bir teşvik modeli sağlar. Bu sistem gnutella ağı içerisinde limeware uygulamasında uygulanmıştır. Böylece kullanıcının, sorguladığı dosyanın gerçekten aradığı şey olup olmadığına karar vermesine ve dosyaları indirmeden değerlendirmesine olanak sağlanmıştır.

Buradaki içerik kirliliği tanımlanmış, belirtilen içeriğe sahip olmayan her şey olarak tanımlanmıştır. Bu modeli ortaya koyan yazara göre, içeriğin kirliliği olup olmadığını değerlendirmede en etkin yol, matematiksel ve istatistiksel yöntemlere oranla dürüst kullanıcılarıdır. Credence yaklaşımında kullanıcı, dosyayı/içeriği indirdikten sonra tek bir oy hakkına sahip olur. Doğru dosya için pozitif, yanlış dosya için negatif oy verilir. Oylar inkar edilememe ilkesi (*non-repudiation*) gereği ve çoklu kimlik oluşturma saldırılarına karşı sayısal olarak imzalanır. Sistem, bu imzalı oyları kullanarak dosyanın oylama sonucunu hesaplar. Uygulamada bir arama olduğunda, o dosya için geçmişte verilen oylardan belli bir miktarı rastgele seçilerek indirilir ve hesaplama sonucu kullanıcıya gösterilir. Böylece kullanıcılar, dürüstlüğü teşvik edilir. Sistemin dezavantajı olarak daha önceden uzun süre dürüst olan bir kullanıcı davranışını değiştirip yalan söylerse küçük bir küme için sonuçları etkileyebilir.

Incentive Cooperation In Peer-To-Peer Networks[16]

Bu çalışmada yazarlar, P2P sistemlerde bedavacılık problemini engelleyebilmek ve sistemin yararını artırabilmek için, evrimsel mahkumlar çıkmazı yaklaşımını kullanarak bir teşvik modeli geliştirmişlerdir. Normal, simetrik bir mahkumlar çıkmazı probleminde işbirliği için, tekrarlı işlem ve ün gerekli iken P2P sistemlerde bu varsayım pek gerçekçi olmayabilir. Çünkü büyük çaplı P2P sistemlerde aynı kullanıcı ile tekrar işlem yapma olasılığı azdır ve kullanıcıların kimlik değiştirme maliyeti sıfır olduğundan kötü ün oluşması olasılığı sıfıra yakındır. Bu nedenle yazarlar simetrik mahkumlar çıkmazı problemini, P2P sistemlerde kullanılacak şekilde genelleştirmişlerdir. Yazarların bulguları şunlardır:

- Bir eşin sadece kendisinin tuttuğu bilgiye dayalı olan teşvik modelleri, sistem büyüklüğü arttıkça çalışmaz.
- Eşlerin tuttuğu bilgileri birbirleri ile paylaştığı teşvik modelleri sistem büyüklüğünden daha az etkilendirir. Ancak dağıtık bir altyapı gerektirir ve birden fazla eşle yapılan saldırılardan etkilenirler.

- Yabancı (daha önce bilinmeyen) eşleri sisteme dahil edebilen teşvik sistemleri, tam bir işbirliği sağlarlar.

A Game Theoretic Framework For Incentives In P2P Systems [18]

Yazarlar bu makalede, eşlerin etkileşimini modellemek için en iyi aracın teorik modelleme olduğuna karar vermişler ve müteakabiliyet tabanlı bir teşvik modeli oluşturmak için Nash dengesinden ve oyun teorisinden faydalanmışlardır. P2P sistemde her eşin kendi faydasını maksimize edeceği düşünülmüştür. Kullanıcının sağladıkları katkı çeşitli şekillerde tutulabilir. Örneğin sisteme sağlanan katkıyı gösteren itibar bunlardan birisi olabilir. Yazarların önerdiği fark modelinin temelini, her eşin kullandığı sistem kaynakları (benefit) ve sağladığı kaynaklar (cost) arası fark oluşturur.

B. Mikro Ekonomi Tabanlı Yaklaşımlar

Mikro ekonomi tabanlı şemalarda, kullanıcılar diğer eşlerin sağladığı servislerden faydalanmak için sanal paralar ödemek zorundadırlar. Böylece sanal bir para ekonomisi kurulmaya çalışılır. Sisteme yapılan her bir katkı için bir sanal para alınırken, sistemden yararlanmak için para ödenir. Eğer İnternet servis sağlayıcıya indirme ve yükleme için ayrı ücretler ödeniyorsa, alınan hizmet ile verilen hizmet gerçekte eşit değildir. Para şeması bunu dikkate alarak tasarlanmalıdır. Bir kere kullanılan paranın tekrar kullanılmasını sağlamak, sahte para üretimini engellemek genelde en önemli problemlerdir. Bu problemi aşmak amacıyla eğer bir merkezi bankaya dayalı model oluşturulursa ölçeklenebilirlik zordur. Merkezi yapıdan biraz ödün vererek yönetici eşler seçilmesi veya bir eşin etrafındakiler için yönetici olması, merkezi bir bankadaki darboğazı çözmek için kullanılabilecek bazı yöntemlerdir. Mikro ekonomi yaklaşımını temel alan bazı yaklaşımları şöyle özetleyebiliriz.

KARMA [13]

Karma [13], bir sanal para şeması kullanarak, kullanıcıların sisteme katkı sağlamasını amaçlar. Genel ekonomi gibi, sistemden bir kaynak bekleyen kullanıcı sanal para ödemek zorundayken, sisteme katkı sağlayan para kazanır. KARMA, bir kullanıcının sisteme sağladığı katkıları ve sistemden aldığı yararları takip ederek bedavacılarla savaşıyor. Her bir kullanıcının performansı karma denilen bir para birimiyle takip edilir. Sisteme ilk katılan kullanıcılara belli bir başlangıç karması (*initial seed karma*) verilir. Bir kaynak indirmek isteyen bir kullanıcının yeterli parası yoksa, o kullanıcıya indirme için izin verilmez. Böylece kullanıcılar sisteme katkı yaparak karma kazanmaya zorlanır. KARMA sistemi, banka olarak bir otoriteye ihtiyaç duymaz. Karma'lar kullanıcının banka kümesi (*bank-set*) denilen bir grup eş tarafından tutulur. Ayrıca hata dayanıklılık için yedekleme (*replication*) ve karma değerlerinin rüşvetle el değiştirmemesi için güvenlik önlemleri kullanılır. KARMA tasarımında sistemde en az k eş olduğu ve bunların belli bir kesiminin dürüst (*non-malicious*) olduğu kabul edilmiştir. Banka kümesi bilgisi, her bir eşin bir banka kümesi ile eşleştirildiği bir dağıtık hash tablosu (Distributed Hash Table) [14] ile tutulur. Her bir A eşinin en yakınındaki k adet eş, A'nın banka kümesini (*bank A*) oluşturur. A eşinin banka kümesi olan her bir eş, A'nın gizli anahtarı ile

imzalanmış karma değerlerini tutar ve A'nın yaptığı işlemlerin geçmişini tutar. Eşlerin karmalarını kullanıp sistemi terk etme durumunda veya karmalarını artırıp sistemi terk etme durumunda oluşacak enflasyon ve denflasyon ile başa çıkmak için para ayarlamaları belli zaman aralıkları (*epoch*) ile yapılır. Karma sistemi, sisteme bir eş katıldığında onun sahip olduğu dosyaların id bilgisi ile eşin id bilgisini eşleştirir. Bir eş, bir dosyayı indirmek istediğinde o dosyaya sahip eşlerin listesini elde eder ve en düşük veya en düşük 2. açık artırma teklifini yaparak (*vickey auction*) indireceği eş seçer. İndirilecek eş seçildikten sonra takas boyunca borç/kredi tutarsızlığını geçici olarak tolere eden ve Bizans oybirliği protokolünü kullanan KARMA takas protokolü başlatılır. Bu protokol şöyledir:

A eşi B eşine, bank A'nın B'ye istenilen ücreti ödemesini gösteren imzalanmış mesajı yollar. B eşi, bunu bank B'ye iletir ve böylece A eşinden B eşine karma transferi başlar. Eğer A eşinde yeterli bakiye varsa, ücret A'dan düşülüp B'nin hesabına aktarılır. Buradaki tüm mesajlar inkar edilememe ve diğer risklere karşı imzalanmış mesajlardır. KARMA'nın ana avantajı, her bir kullanıcıyı takip etmesi nedeniyle, kullanıcıları katkıları ile tüketimleri arasında bir denge kurmaya zorlar. Ancak her bir kullanıcının, başka bir kullanıcı için bankacı rolünü üstlenmesi gereklidir. Bunun için ise bir teşvik yoktur. Ayrıca KARMA çoklu kimlik tanımlama saldırılarına karşı dirençsizdir.

Incentive For Sharing In Peer-To-Peer Networks [15]

Bu makalede yazarlar, P2P ağlarda bedavacılık problemi ile başa çıkabilmek için formal bir oyun teorisi modeli kurmuşlar ve çeşitli mikro ekonomi modelleri altında bu kullanıcıların dengesini analiz etmişlerdir. Kurdukları modelde kullanıcıların kendi faydalarını maksimize etmek için bencil davranacaklarını varsaymışlar ve buna göre sisteme çeşitli ekonomi modelleri ekleyip kullanıcıların davranışlarını analiz etmişlerdir. Kurdukları teşvik modelinde bir ajanın yaptığı toplam indirme sayısı ve toplam paylaşım sayısını içine alan bir ücret hesaplamışlardır. Buna göre her bir eşin herhangi bir anda 2 etkinliği olabilir: paylaşım ve indirme. Bu iki olayda az, orta, veya çok olarak 3 ayrı dereceye ayrılmıştır. Ayrıca her bir eşin faydası, çeşitli parametrelere dayalı bir fonksiyon olarak yazılmış ve böylece çeşitli durumlar altındaki eşlerin tercihi parasal olarak hesaplanmaya çalışılmıştır.

Yazarlar Napster sistemini incelemiş ve herhangi bir teşvik modeli olmaması nedeniyle kendi modellerini uygulamak için bu sistemi kullanmışlardır. Napster sisteminde teşvik olarak, topluluklarda paylaşım örgütlenmiş ve öntanımlı uygulama ayarlarında paylaşım yapma ayarı kurulmuştur. Böylece sistemde fedakâr kullanıcılar olması sağlanmıştır.

Enforcing Fair Sharing of Peer-To-Peer Resources [17]

Bu çalışmada yazarların amacı, bir eşin kendi paylaşım yaptığı kadar indirme yapabilmesini sağlayan bir adil paylaşım sistemi oluşturabilmektir. Merkezi otorite durumundaki bir eş tüm işlemleri gözlemleyerek bunu sağlayabilir. Fakat bu yöntem kullanılırsa, büyük bir sistemde performans sorunu ve hataya duyarlı tek bir nokta olacağı aşikârdır.

Yazarlara göre P2P sistemlerde teşvik modelini kırmamanın ve sistemden daha fazla indirme yapmanın 3 çeşit durumu vardır:

- İşbirliği Olmadan: Bir eşin, ağdan daha fazla yararlanmak için kendi kendine açıklar bulmaya çalışmasıdır. Bu durumda iş birliği yapabileceği bir eş bulamamıştır.
- Azınlık İşbirliğiyle: Bir grup eşin gizli olarak anlaşarak, kaynak paylaşımları konusunda yalan söylemeleri ve böylece sistemde daha çok paylaşım yapmış gibi görünmeleridir.
- Rüşvetle: Kötü niyetli eşlerin bazı eşleri seçerek, sistemi kandırmak üzere onları ikna etmeye çalışmasıdır.

Bu çalışmada ilk olarak işbirliği olmadan yapılan saldırılara odaklanılmıştır. Kaynak tüketimi bir çeşit parasal işlem olarak düşünülmüş ve kendi kaynağımızın dışındaki kaynaklar her zaman daha çok pahalı olarak belirlenmiştir. Böylece paylaşım yapmak her zaman daha getirili bir işlem olmuştur. Eğer iki eş kendi aralarında bir şeyler paylaşıyorsa, bu işlem için parasal ücret sıfır kabul edilmiştir.

Yazarların asıl tasarımları, eşlerin yaptıkları tüm işlemleri bir şekilde kayıt altında tutmayı sağlamaktır. Bunun için 3 çeşit tasarım önermişlerdir. Bu tasarımlarda, her eşin bir açık anahtar çifti ile sayısal imzalama yapabildiği varsayılmıştır. Ayrıca bir mesaj özeti (*hash digest*) ile dosyaların gerçekten o eş üzerinde olup olmadığının anlaşılması sağlanmıştır.

Yazarların ilk önerdikleri tasarım, akıllı kart (*smart cards*) kullanımınıdır. Bu yöntemle eşler, istekleri için ücretleri akıllı kart ile onaylatacak ve isteğini elde edecektir. Fakat, güvenilir bir otorite olmadığı ve geçerliliğini yitirmiş kartların problem olması nedeniyle P2P sistemlerde uygulanabilir görülmemiştir.

İkinci tasarım ise kota (*quota*) yöneticilerdir. Bu yöntemde, bir eşe komşu olan bir grup eş, o eşin kota yöneticisi olarak belirlenmiştir. Her bir yönetici, yönettiği eşin ne kadar veri tükettiğini ve eşden gelen istekleri onaylamak ile görevlendirilmiştir. Azınlık işbirliğini çözmek için yönetici eşler, Bizans oybirliği protokolünü uygulayarak isteğin geçerliliğini kontrol ederler. Bu yöntemin kötü yanı, her bir istek için onay gerektiği için gecikme olması (*latency*) ve kötü niyetli eş sayısının kümenin üçte birinden az olması gerektiğidir. Ayrıca reddedilmesi gereken bir isteğe izin veren bir yönetici için hiçbir ceza olmadığından, bu yaklaşım rüşvet saldırılarına karşı savunmasızdır.

Üçüncü tasarım ise her eşin sayısal olarak imzalanmış bir kullanım dosyası tutmasıdır. Bu dosyada üç çeşit bilgi vardır: sisteme sağlanan katkı (yüklemeler), gönderilenler listesi (hangi eşe hangi dosyanın gönderildiği), indirilenler listesi (hangi dosyaların indirildiği). Gönderilenler listesi ile indirilenler listesi bir eşin alacaklarını ve borçlarını anlatır. Eğer bir eşin indirdikleri yüklediklerini aşmamış ise indirme yapabilir. Bu yaklaşımda, eşlerin yalan söylememesi için imzaya dayalı önlemler alınmıştır.

V.SONUÇ

P2P sistemler kendi kendine organize olan, merkezi olmayan, dağıtık ağlardır. Herhangi bir yönetici olmaması, kontrol olmaması, dinamik olarak büyüyüp küçülmesi, dağıtık veri depolama ve paylaşma için mükemmel imkanlar sunmaktadır. Fakat P2P sistemlerin demokratik (veya anarşik) yapısının yolaçtığı bazı zararlar da vardır. Merkezi bir otoritenin olmaması, kullanıcıların sisteme katkı yapmamasına yol açar. Paylaşım için gönüllülük esasının olması, sistem kaynaklarını değişken ve tahmin edilemez

yapar. Napster, Gnutella gibi sistemler üzerinde yapılan araştırmalara göre, kullanıcıların büyük çoğunluğu sisteme katkı sağlamamakta ve sisteme sadece tüketici olarak katılmaktadır. Bu nedenlerle, P2P sistemler üzerinde eşleri, paylaşımaya zorlayacak teşvik modellerine ihtiyaç vardır.

Bu çalışmada, P2P sistemlerdeki teşvik modelleri incelenmiştir. Genelde çoğu teşvik modeli, oyun teorisini temel alarak oluşturulmaya çalışılmıştır. Oyun teorisinde temel amaç, kullanıcılar arasında bir denge fonksiyonu tanımlayabilmek ve sistemin kullanıcılarını buna uyacak şekilde modellemektir. Halihazırda, mütekabiliyet tabanlı ve mikro ekonomi tabanlı yaklaşımları kullanan teşvik modelleri göze çarpmaktadır. Mütekabiliyet tabanlı modellerde, her bir eş, kendi sakladığı geçmiş paylaşım bilgilerini veya etrafındaki diğer eşlerin sakladığı bilgileri kullanarak, indirme istemleri konusunda karar vermeye çalışmaktadır. Mikro ekonomi yaklaşımlarında ise, genelde bir para birimi oluşturulmakta ve bu para ile eşler birbirlerinden hizmet isteminde bulunmaktadırlar. Böylece sanal bir ekonomik düzen oluşturulmaya çalışılmaktadır.

Gelecekte P2P sistemlerde üzerinde bu alanda yapılabilecek çalışmalarda, itibara dayalı güven modelleri yardımıyla teşvik modelleri oluşturmak iyi sonuçlar verebilecek bir yaklaşım olarak görünmektedir. Güven modellerinin topladığı bilgilere ek olarak, paylaşım bilgilerini de toplamak ve bu bilgilerin hepsini teşvik modelinde kullanmak, eşleri sisteme katkı sağlama konusunda zorlayabilecek bir yaklaşımdır. Böylelikle günlük hayatta daha uygulanabilir, kötü niyetli kullanıcıları da engelleyen teşvik modelleri geliştirmek mümkün görünmektedir.

KAYNAKLAR

- [1]. E. Adar and B. Huberman. Free riding on gnutella, 2000
- [2]. S. Saroiu, P. K. Gummadi, S. D. Gribble, A Measurement Study of Peer-to-Peer File Sharing Systems, Proc. of Multimedia Computing and Networking 2002 (MMCN '02)
- [3]. John R. Douceur. The sybil attack. In IPTPS '01: Revised Papers from the First International Workshop on Peer-to-Peer Systems, pages 251–260, London, UK, 2002. Springer-Verlag.
- [4]. James Andreoni. Giving with impure altruism: Applications to charity and ricardian equivalence. *The Journal of Political Economy*, 97(6):1447–1458, 1989.
- [5]. M. Feldman, C. Papadimitriou, J. Chuang, and I. Stoica. Free-riding and whitewashing in peer-to-peer systems. *Selected Areas in Communications, IEEE Journal on*, 24(5):1010–1019, May 2006
- [6]. Seung Jun and Mustaque Ahamad. Incentives in bittorrent induce free riding. In P2PECON '05: Proceedings of the 2005 ACM SIGCOMM workshop on Economics of peer-to-peer systems, pages 116–121, New York, NY, USA, 2005. ACM
- [7]. Kevin Walsh and Emin Gun Sirer. Experience with an object reputation system for peer-to-peer filesharing. In NSDI'06: Proceedings of the 3rd conference on 3rd Symposium on Networked Systems Design & Implementation, pages 1–1, Berkeley, CA, USA, 2006. USENIX Association.
- [8]. Bram Cohen. Incentives build robustness in bittorrent, 2003.
- [9]. Michael Piatek, Tomas Isdal, Thomas Anderson, Arvind Krishnamurthy, and Arun Venkataramani. Do incentives build robustness in bittorrent? In NSDI'07, Cambridge, MA, April 2007.
- [10]. Dongyu Qiu and R. Srikant. Modeling and performance analysis of bittorrent-like peer-to-peer networks. In SIGCOMM '04: Proceedings of the 2004 conference on Applications, technologies, architectures, and protocols for computer communications, pages 367–378, New York, NY, USA, 2004. ACM.
- [11]. Lei Guo, Songqing Chen, Zhen Xiao, Enhua Tan, Xiaoning Ding, and Xiaodong Zhang. Measurements, analysis, and modeling of bittorrent-like systems. In IMC'05: Proceedings of the Internet Measurement Conference 2005 on Internet Measurement Conference, pages 4–4, Berkeley, CA, USA, 2005. USENIX Association.
- [12]. Larry Peterson, Tom Anderson, David Culler, and Timothy Roscoe. A Blueprint for Introducing Disruptive Technology into the Internet. In Proceedings of HotNets–I, Princeton, New Jersey, October 2002.
- [13]. Vivek Vishnumurthy, Sangeeth C handrakumar, and Emin Gun Sirer. Karma: A secure economic framework for p2p resource sharing. In Workshop on the Economics of Peer-to-Peer Systems, Berkeley, California, 2003.
- [14]. Ion Stoica, Robert Morris, David Liben-Nowell, David R. Karger, M. Frans Kaashoek, Frank Dabek, and Hari Balakrishnan. Chord: a scalable peer-to-peer lookup protocol for internet applications. *IEEE/ACM Trans. Netw.*, 11(1):17–32, 2003
- [15]. Philippe Golle, Kevin Leyton-Brown, Ilya Mironov, and Mark Lillibridge. Incentives for Sharing in Peer-to-Peer Networks, Computer Science Department, Stanford University, 2001
- [16]. Kevin Lai, Michal Feldman, Ion Stoica, and John Chuang. Incentives for Cooperation in Peer-to-Peer Networks, Computer Science Division U.C. Berkeley, School of Information Management and Systems U.C. Berkeley, 2003
- [17]. [17] Tsuen-Wan “Johnny” Ngan, Dan S. Wallach, and Peter Druschel. Enforcing Fair Sharing of Peer-to-Peer Resources, Department of Computer Science, Rice University, 2003
- [18]. Chiranjeev Buragohain, Divyakant Agrawal, Subhash Suri, A Game Theoretic Framework for Incentives in P2P Systems, Computer Science Department University of California Santa Barbara, CA 93106, 2003
- [19]. Hardin, G. (1968). "The Tragedy of the Commons". *Science* 162 (3859): 1243–1248.
- [20]. R. J. Aumann ([1987] 2008). "game theory," Introduction, *The New Palgrave Dictionary of Economics*, 2nd Edition. Abstract.
- [21]. Roger B. Myerson (1991). *Game Theory: Analysis of Conflict*, Harvard University Press, p.
- [22]. Nash, John (1950), "Equilibrium points in n-person games", *Proceedings of the National Academy of Sciences of the United States of America* 36 (1): 48–49
- [23]. Axelrod, Robert. *The Evolution of Cooperation*. New York: Basic Books, 1984.
- [24]. E. Friedman and P. Resnick, "The social cost of cheap pseudonyms," *J. Econ. Manage. Strategy*, vol. 10, no. 2, pp. 173–199, 1998. [Online]. Available: citeseer.nj.nec.com/friedman98social.html
- [25]. P. Resnick, K. Kuwabara, R. Zeckhauser, and E. Friedman, "Reputation systems," *Communications of ACM*, vol. 43, no. 12, pp. 45–48, 2000.
- [26]. S. Kamvar, M. Schlosser, and H. Garcia-Molina, "The eigentrust algorithm for reputation management in p2p networks," in *Proceedings of the 12th World Wide Web Conference (WWW)*, 2003