EŞLER ARASI AĞLARDA GÜVEN TABANLI TEŞVİK MODELİ

TRUST-BASED INCENTIVE MODEL IN PEER-TO-PEER NETWORKS

SERKAN ÇAKMAK

YRD. DOÇ. DR. AHMET BURAK CAN
Tez Danışmanı

Hacettepe Üniversitesi
Lisansüstü Eğitim – Öğretim ve Sınav Yönetmeliğinin
Bilgisayar Mühendisliği Anabilim Dalı İçin Öngördüğü
YÜKSEK LİSANS TEZİ
olarak hazırlanmıştır.

2014

Serkan ÇAKMAK'ın hazırladığı **"Eşler Arası Ağlarda Güven Tabanlı Teşvik Modeli"** adlı bu çalışma aşağıdaki jüri tarafından **BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI**'nda **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Doç. Dr. Süleyman TOSUN
Başkan :. . . . . .

Yrd. Doç. Dr. Ahmet Burak CAN
Danışman :. . . . . .

Yrd. Doç. Dr. Kayhan İMRE
Üye :. . . . . .

Yrd. Doç. Dr. Murat AYDOS
Üye :. . . . . .

Yrd. Doç. Dr. Mehmet DEMİRCİ
Üye :. . . . . .

Bu tez Hacettepe Üniversitesi Fen Bilimleri Enstitüsü tarafından **YÜKSEK LİSANS TEZİ** olarak onaylanmıştır.

Prof. Dr. Fatma SEVİN DÜZ
Fen Bilimleri Enstitüsü Müdürü

Her zaman yanımda bulunan herkese..

ETİK

Hacettepe Üniversitesi Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu,
- başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
- atıfta bulunduğum eserlerin tümünü kaynak olarak gösterdiğimi,
- kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- ve bu tezin herhangi bir bölümünü bu üniversite veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı

beyan ederim.

. . . . . /. . . . . /. . . . . .

Serkan ÇAKMAK

ÖZET

EŞLER ARASI AĞLARDA GÜVEN TABANLI TEŞVİK MODELİ

Serkan ÇAKMAK
Yüksek Lisans, Bilgisayar Mühendisliği Bölümü
Tez Danışmanı: Yrd. Doç. Dr. Ahmet Burak CAN
Ekim 2014, 87 Sayfa

Eşler arası ağlar, kaynak paylaşımı, yönlendirme ve kaynak arama gibi görevlerde eşlerin katkı sağlaması ilkesine göre çalışır. Sisteme katkı sağlayan eş sayısı ne kadar fazla ise sistemin başarısı da o derece yüksektir. Eğer eşlerin bir kesimi, sisteme bu görevlerde katkı sağlamazsa, sistem verimliliği ve etkinliği önemli zarar görür. Bu durum bedavacılık(free-rider) olarak da bilinen problemdir. Bu bedavacılık problemi ile baş edebilmek ve sistemdeki her eşin katkı yapmasını sağlamak için teşvik modelleri geliştirilmiştir. Teşvik modelleri sistemdeki her bir eşin sisteme katkı yapmasını sağlatan modellerdir. Genel amaçları sisteme katkı yapmayan eşlerin sistemden fayda sağlamasını engelleyerek sadece sisteme katkı yapan eşlerin fayda sağlamasını sağlamaktır.

Yapılan tez çalışması kapsamında eşler arası sistemlerde güven modeli tabanlı bir teşvik modeli geliştirilmiştir. Güven modeli kapsamında toplanan

metrikler kullanılarak geliştirilen bu teşvik modeli ile bedavacılık, geçmişi silme, çoklu kimlik tanımlama problemleri çözülmeye çalışılmış ve güven modellerinin teşvik için de kullanılabileceği gösterilmiştir. Geliştirilen model çeşitli saldırgan tipleri için test edilmiş ve başarılı sonuçlar elde edilmiştir.

ANAHTAR SÖZCÜKLER: Bilgisayar Ağları, Eşler Arası Ağlar, Teşvik Modelleri, Bedavacılık, Geçmişi Silme, Çoklu Kimlik Tanımlama, Güven Modelleri

ABSTRACT

A TRUST BASED INCENTIVE MODEL IN PEER-TO-PEER NETWORKS

Serkan ÇAKMAK

Master of Science, Department of Computer Engineering

Supervisor: Asst. Prof. Dr. Ahmet Burak CAN October 2014, 87 Pages

Peer-To-Peer networks work by relying on involvement of peers on tasks like resource sharing, routing, and querying of resources. Power of peer-to-peer systems come from resource sharing. If some peers do not contribute to the system, efficiency and effectiveness of the system is degrades. This situation is expressed as free-riding problem. To cope with free-riding and encourage all peers to contribute, incentive models are developed. Incentive models basically aim to encourage all peers to contribute. Main purpose of incentive models is to prevent peers which do not contribute to system and only allow peers which contribute to system for getting services.

Within the context of this thesis, a trust based incentive model is developed. Free-riding, white washing, and sybil attack are aimed to solve with this model which uses some metrics gathered as part of trust model. The

proposed model has shown that trust models can be used to provide incentives. The model trained for different situations and attack types are tested in various configurations and successful results are obtained.

KEYWORDS: Network, P2P Networks, Incentive Models, Free-Riding, White Washing, Sybil Attack, Trust Models

TEŞEKKÜR

Tez konusunun belirlenmesinde ve tez süresince tez ile ilgili bildiri ve tez metni konusundaki düzenlemelerinde büyük yardımı olan ve vaktini ayıran hocam Sayın Yrd. Doç. Dr. Ahmet Burak CAN'a,

Tez metnini inceleyerek biçim ve içerik bakımından son halini almasına yardımcı olan Sayın Doç. Dr. Süleyman TOSUN'a, Sayın Yrd. Doç. Dr. Kayhan İMRE'ye, Sayın Yrd. Doç. Dr. Murat AYDOS'a ve Sayın Yrd. Doç. Dr. Mehmet DEMİRCİ'ye,

Gerek tez metnini biçim bakımından inceleyerek gerek de bana sürekli destek vererek yardımcı olan Gözde BATMAZ'a,

Lisans ve yüksek lisans boyunca çok değerli bilgiler öğrendiğim üzerimde emeği geçen tüm hocalarıma,

Manevi desteğini ve fikirlerini esirgemeyerek daima destek olan değerli dostlarıma ve arkadaşlarıma,

Her koşulda beni destekleyen ve daima yanımda olan sevgili aileme,

teşekkür ederim.

İÇİNDEKİLER

ŞEKİLLER

ÇİZELGELER

SİMGELER VE KISALTMALAR

P2P Peer-to-peer
DHT Distributed hash table
GT Güven Tabanlı
GTU Güven Tabanlı Uyarlanabilir

ALGORİTMALAR

1 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 yönetimin ve hataya duyarlı tek bir nokta (single point of failure) durumunun olduğu net bir biçimde görülmektedir. Ayrıca, her istemcinin indirme hızı, sunucunun paylaşılan yükleme 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.

Merkezi otoritenin olmaması ve her kullanıcının hem istemci hem de sunucu olma durumu getirdiği avantajların yanında bazı olumsuz sonuçlar da doğurmuştur. Merkezi otorite boşluğu kontrol edilebilirliği azaltmış, sisteme katılan kötü niyetli kullanıcıların herhangi bir ceza ile karşılaşmadan istediklerini yapabilmelerine olanak sağlamıştır.

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 bırakmaktadırlar [2]. Bu durum, ağın etkinliğini ciddi ölçüde etkilemekte ve bazı eşlere fazla yük binmesine sebep olabilmektedir. Bu nedenle, ağ üzerindeki bütün eşleri sisteme katkı sağlamaya motive etmek ve bazen de

zorlamak üzere teşvik 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.

Teşvik modelleri genel olarak her bir kullanıcı ve/veya kullanıcı grupları hakkındaki bilgileri değerlendirerek kullanıcıların sistemden fayda sağlamalarına izin verir. Teşvik modelleri, adından da anlaşılacağı üzere her bir kullanıcıyı sisteme katkıda bulunmak üzere çeşitli şekillerde teşvik eder. Sisteme katkıda bulunmadan sadece sistemden yararlanmaya çalışan kullanıcıları ise engeller. Güven modelleri ise, sistemde çeşitli şekillerde zararlı paylaşımda bulunarak diğer iyi niyetli kullanıcılara zarar vermek isteyen kötü niyetli kullanıcıları engellemeye çalışan modellerdir. Bu modeller bir kullanıcının bir sunucu eş seçimi esnasında kullanılarak istemci eşin en güvenilir ve en uygun sunucu eşi belirlemesini sağlamayı amaçlarlar.

Eşler arası sistemlerde, denetimden bağımsız bir şekilde sisteme giriş imkanının olması, her tür kullanıcının hem istemci hem sunucu olması, kullanıcıların istedikleri zaman sistemden ayrılıp aynı şekilde istedikleri zaman sisteme dahil olma olanakları teşvik ve güven modellerinin gerçekleştirimini zorlaştıran etmenlerin başlıcalarıdır. Bir teşvik veya güven modeli geliştirilirken, sistemin başarısı açısından, mutlaka iyi niyetli kullanıcılar teşvik sisteminden en az şekilde etkilenmelidir.

Bu tez kapsamında, güven modeli tabanlı bir teşvik modeli oluşturulmuş ve gerçekleştirilmiştir. Oluşturulan model ile birlikte günlük yaşama uygun çeşitli saldırgan tipleri de geliştirilmiş ve bu saldırgan tipleri ile modelin benzetimi yapılmıştır. Modelde her bir kullanıcının sisteme sağladığı fayda ve sistemden aldığı fayda ölçülmüş ve saklanmıştır. Ayrıca güven modeli kapsamında her bir kullanıcının, etkileşimde bulunduğu diğer kullanıcılara ilişkin etkileşim sonuçları kullanıcı tarafından değerlendirilmiş

ve bu değerler de saklanmıştır. Saklanan bu tüm değerler, bir istemci rolündeki kullanıcı, sunucu rolündeki kullanıcıdan bir servis istediğinde, sunucu rolündeki kullanıcı tarafından kullanılmış ve teşvik modeli yardımıyla istemci kullanıcının nasıl bir türde kullanıcı olduğunu tahmin etmede girdi olmuştur. İstemci kullanıcıya teşvik modelinin istediği nitelikleri sağlaması durumunda servis sağlanmış; diğer durumlarda ise istemci kullanıcı reddedilmiştir. Oluşturulan model üç aşamalı olarak geliştirilmiş ve en son aşamada en iyi sonuçlar elde edilmiştir. Modelde ilk olarak basit düzeyde her bir kullanıcının indirdiği ve gönderdiği veri miktarları kayıt altına alınmış ve bir kullanıcının indirme yapabilmesi için o kullanıcının gönderme veri miktarı ile indirme veri miktarının oranı sistemdeki eşik değer ile karşılaştırılmıştır. İkinci aşamada güven değerleri de teşvik model kapsamında kullanılmış ve bir kullanıcının indirme yapabilmesi için hem gönderme veri miktarı ile indirme veri miktarının oranı sistemdeki eşik değerden büyük olması hem de kullanıcının güven değerinin eşik güven değerinden büyük olması zorunluluğu getirilmiştir. Son olarak model de sabit bir eşik değer yerine kullanıcının davranışına göre belirlenen uyarlanabilir bir eşik değeri tanımlanmış ve bu model ile birlikte en iyi sonuçlar elde edilmiştir.

Tez içeriği genel olarak şu şekildedir: Bölüm 2'de eşler arası sistemlerin genel yapısı ve türleri anlatılmıştır. Bölüm 3'te itibar ve güven tanımlanarak eşler arası sistemlerdeki güven, teşvik modellerinden ve bu kapsamda yapılmış çalışmalardan bahsedilmiştir. Bölüm 4'te geliştirilen model ile ilgili kabuller ve modelin kendisi anlatılmıştır. Bölüm 5'te, tez kapsamında geliştirilen benzetim modülünden, saldırgan türlerinden ve modelin benzetim sonuçlarından bahsedilmiştir. Bölüm 6'da ise yapılan çalışmaların ve modelin özetleri anlatılarak tez sonuçlandırılmıştır.

2 EŞLER ARASI SİSTEMLER

Eşler arası sistemler, istemci-sunucu mimarisine bir alternatif olarak ortaya çıkan bir ağ yapısıdır. İstemci-sunucu mimarisinde her zaman tek bir sunucu ve bu sunucudan isteklerde bulunan istemciler bulunmaktadır. Sunucu sahip olduğu veri gönderme bant genişliğini istemciler arasında paylaştırır. Bu tip sistemlerde istemci sayısı için sunucunun destekleyebileceği bir limit de bulunmaktadır.

Klasik yapıdaki bu ağ sistemlerinin aksine, eşler arası ağlarda herhangi kesin bir istemci ve sunucu rolü bulunmamaktadır. Herhangi bir kullanıcı (*peer*) aynı veya farklı anlarda hem sunucu hem de istemci rolünü üstlenebilir. Böyle bir yapının en önemli avantajı sistemde herhangi bir bant genişliği veya istemci sayısı sınırı olmamasıdır. Ayrıca eşler arası sistemler kullanıcıların sistemden ayrılmaları veya sisteme dahil olmaları bakımından dinamik bir yapıya sahiptir.

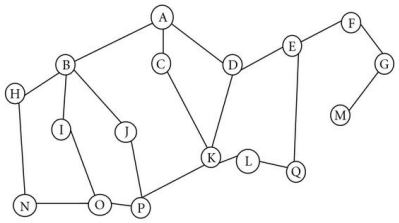
Eşler arası ağlar yapısal olarak incelendiğinde üç ana gruba ayrılabilir. Bunlar yapısal olmayan eşler arası ağlar, yapısal eşler arası ağlar ve hibrit eşler arası ağlardır.

2.1 Yapısal Olmayan Eşler Arası Ağlar

Yapısal olmayan eşler arası ağlar herhangi bir merkezi otoritenin olmadığı ve tüm kullanıcıların eşit olduğu bir sistemdir. Bu sistemlerde her kullanıcı aynı rolleri üstlenirler. Yapısal olmayan eşler arası ağlar dinamiklik özelliği ile ön plana çıkmaktadır. Sisteme katılmak ve sistemden ayrılmak çok az maliyetli bir işlemdir. Örneğin, bir arazi üzerinde rastgele hareket halinde bulunan sensörlerden oluşan bir ağ sisteminde veri iletimi ve paylaşımı yapısal olmayan eşler arası ağlar ile gerçekleştirilir. Eşlerin sistemden sık sık ayrılmaları ve tekrar katılmaları bu tip bir sistemde herhangi bir soruna

yol açmaz.

Yapısal olmayan eşler arası ağlar sisteme dahil olma ve sistemden ayrılma işlemlerinde avantajlar sağlasa da, sistemdeki bir içeriği arama işleminde dezavantajlara sahiptir. Bir kullanıcı herhangi bir içeriği aramak istediğinde, bu işlem ile ilgili sorgu diğer tüm kullanıcılara gönderilmek zorundadır. Ayrıca sorguya olumlu cevap vermesi gereken kullanıcılar sorgu sahibi kullanıcıya cevaplarını göndermek zorundadır. Herhangi bir yapısal altyapı olmadığından, bir sorgu ilk olarak tüm komşulara gönderilir. Aynı şekilde komşularda gelen sorguyu kendi komşularına gönderir. Bu işlem her bir kullanıcı sorguyu alana kadar devam eder. Query flooding [3] olarak bilinen bu yöntem, ağın bant genişliğini olumsuz etkilemekte ve ağ trafiğini artırarak ağın etkinliğini düşürmektedir. Bu problemle başa çıkabilmek arama sorgusunu tüm ağ yerine ağın bir alt kümesine gönderme gibi çözümler öne sürülse de problem tam olarak ortadan kaldırılamamıştır. Bu nedenle içerik arama işleminin yoğun kullanım gerektirdiği durumlarda yapısal olmayan eşler arası ağlar kullanılmamalıdır. Şekil 1 örnek bir yapısal olmayan eşler arası ağı göstermektedir. Şekilde de görüldüğü üzere düğümler topolojik olarak eşittir ve uçtan uca iletişim diğer düğümler yardımıyla gerçekleştirilir. Gnutella [4], en yaygın bilinen yapısal olmayan eşler arası ağdır. Gnutella içerik paylaşmak için oluşturulan herhangi bir yapısal hiyerarşinin bulunmadığı bir ağdır. Kullanıcılar istedikleri zaman ağa dahil olup, ağdan ayrılabilmektedirler. Gnutella ağında arama işlemi flooding işlemine göre yapılır. Ancak Gnutella aramalarda trafiği azaltmak için önceden tanımlı bir arama sorgusu iletimi sınırı belirlemiştir. Sorgu yaşam süresi (*Time-to-Live TTL*) adı verilen bu sistem ile sorgu belirli eş sayısına iletildikten sonra, iletimi sonlanmaktadır. Bu sistem ile ağ trafiği yoğunluğunun tüm sisteme yayılması engellenmiştir.



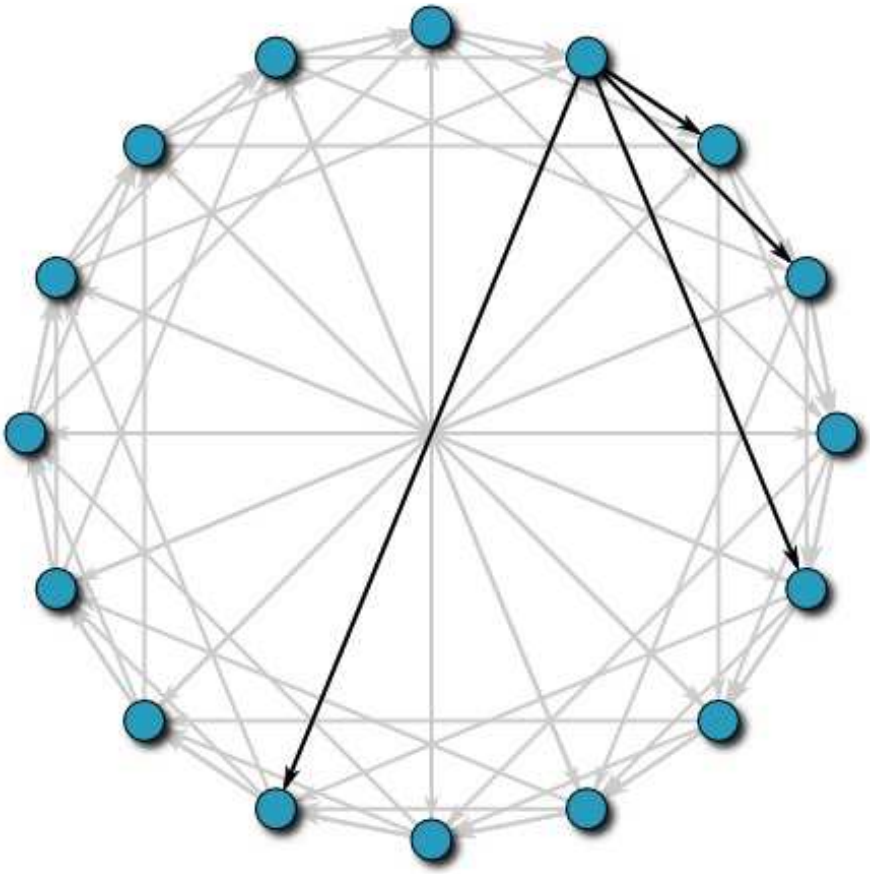
Şekil 1: Örnek Yapısal Olmayan Eşler Arası Ağ

2.2 Yapısal Eşler Arası Ağlar

Yapısal eşler arası ağlar çeşitli topolojik yapılarda oluşturulmuşlardır. Bu topolojik yapılarda diğer eşlerden daha üstün rollerde bulunan çeşitli eşler bulunabilir. Yapısal eşler arası ağlar, yapısal olmayan eşler arası ağlarda içerik arama işleminin etkin yapılamamasından kaynaklı dezavantajları kolayca ve etkin bir şekilde çözebilmek için oluşturulmuşlardır. Bu problemi çözebilmek için her bir eş bulunduğu topolojik yapı ile ilgili bilgiler tutmakta ve ağa katılan veya ağdan ayrılan eşler olması durumunda bu bilgileri güncellemek zorundadır. Böyle bir işlem, ağın dinamikliğini ve sisteme dahil olma, sistemden ayrılma etkinliğini azaltsa da, arama işlemlerinde performansı artırmaktadır.

Çoğu yapısal eşler arası ağ, DHT [5] protokolü kullanarak arama işlemlerinde kolaylık sağlamaktadır. DHT, anahtar-içerik ikililerinden oluşan bir arama tablosudur. Arama yapılacak değer bir çeşit özet (*hash*) metodundan geçirilerek anahtar elde edilir ve bu anahtar ile içerik eşleştirilir. Örneğin bir dosya ile bu dosyaya sahip olan eş listesi aranmak istendiğinde dosyanın tekil kısıtlayıcısı (*id*) bir özet metodundan geçirilerek elde edilen anahtar ile eş listesi eşleştirilir. Herhangi bir eş, dosyaya sahip olan eş listesini aramak istediğinde üreteceği anahtar ile DHT'ye ulaşması yeterlidir. [6, 7, 8] modelleri kendi içlerinde DHT kullanan modellere örnektir.

Chord [9, 10], Tapestry [11], CAN [12] yapısal eşler ağlar arasında en yaygın olarak bilinen bir ağ protokolüdür. N sayıda eşten oluşan bir ağda



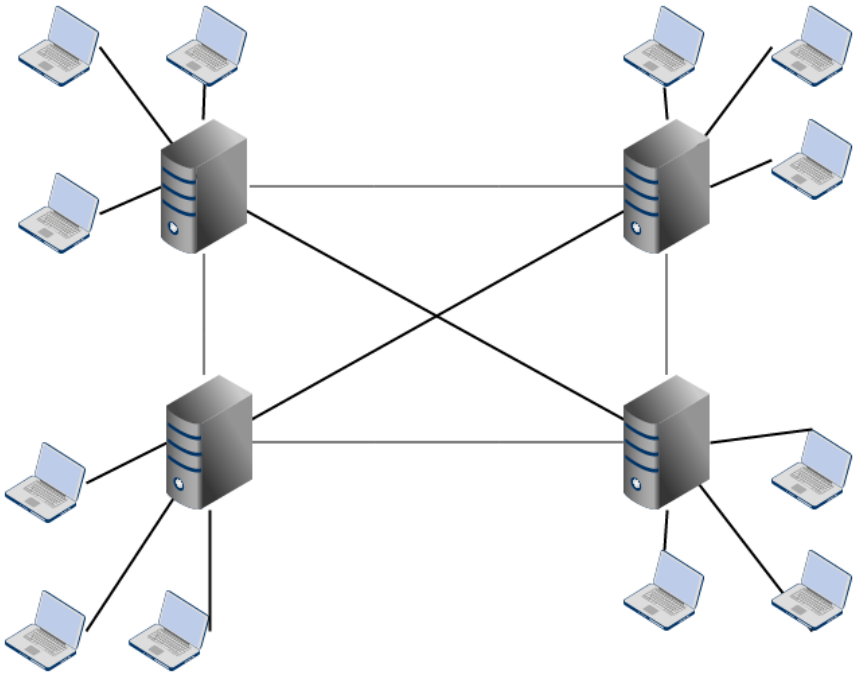
Şekil 2: Chord Ağı [1]

Chord protokolüne göre her bir eş *log N* adet komşu bilgisini finger table adı verilen bir tablo üzerinde saklamak ve ağda meydana gelen değişikliklere karşı güncel tutmak zorundadır. Eşlerin dairesel bir yapıda sıralandığı varsayılan Chord protokolünde, bir işlev ile bir anahtar tahsis etmekte ve işlev, bu anahtar ile ilgili bir kaynağı barındıran bir kullanıcıyı temsil etmektedir. Anahtarların kullanıcıları temsil etmesi için tutarlı özetleme (*consistent hashing* [13]) yöntemi kullanılmaktadır. Bu yöntem sayesinde bir kullanıcı üzerindeki anahtar sayısının dengeli olarak dağıtılması sağlanır. Aramalar bu anahtarlar üzerinden yapılmakta ve sonuçlara göre kaynaklara ulaşılmaktadır. Şekil 2 Chord'un genel yapısını göstermektedir.

2.3 Hibrit Eşler Arası Ağlar

Hibrit eşler arası ağlar, klasik istemci-sunucu mimarisi ile eşler arası ağın birleştirilmesi ile ortaya çıkan yapıdaki ağlardır. Bu ağlarda hem istemci-sunucu mimarisinin hem de eşler arası ağ mimarisinin olumlu yanları birleştirilerek dezavantajlar yok edilmeye çalışılır.

Hibrit yapıdaki ağlarda ağ yapısı içerisine belirli merkezi eşler atanarak arama işlemleri bu merkezi eşler yardımı ile yapılır. Merkezi bir veya bir kaç otoritenin olması güvenlik, arama, yönetim alanlarında avantajlar sağlarken, temeldeki eşler arası ağ prensibi istemci-sunucu mimarisindeki dezavantajları da kapatmaktadır. Spotify [14] hibrit model kullanan bir uygulamadır. Spotify sisteminde içeriğin ilk parçası her zaman sunucudan indirilirken kalan parçalar eşlerden indirilir. Eğer eşlerden yeterli indirme sağlanamaz ise tekrardan sunucudan indirme devam edilir. Günümüzde hibrit modellerin saf istemci-sunucu veya eşler arası ağ mimarilerine göre daha efektif olduğu söylenmektedir [15]. Şekil 3 örnek bir hibrit eşler arası ağın yapısını göstermektedir. Şekilde merkezde yönetici düğümler bulunurken, her bir merkezi düğümün altında uç düğümler bulunmaktadır. Merkezi düğümler sadece kendi altındaki düğümlerden haberdarlardır.



Şekil 3: Örnek Hibrit Eşler Arası Ağ

3 TEŞVİK VE GÜVEN SİSTEMLERİ

3.1 Teşvik

Teşvik kelimesi, sözlük anlamı olarak özendirmek isteklendirmek anlamına gelmektedir. Günümüzde birçok işte, süreçte insanları bir amaca yönlendirmek ve başarıya ulaştırmak için teşvik kullanılmaktadır.

Bir amaca ulaşmak için ödül ve ceza mekanizması teşvikte temel oluşturmaktadır. Ödül mekanizmasında istenilen amaca ulaşılması durumunda, kişilerin istedikleri, değerli gördükleri hediyeler ödül olarak verilirken, ceza mekanizmasında istenilen amaca ulaşılmaması durumunda kişilerin değer verdikleri şeyler ellerinden alınarak ceza verilmektedir. Hayatımızda birçok alanda teşvik işlemini gözlemleyebiliriz. Örneğin bir ebeveynin, kendi çocuğunun başarılı olması durumunda ödül için hediyeler alıp, başarısız olması durumunda ceza vermesi teşvik için bir örnektir.

İnternet ortamında teşvik ile ilgili verebileceğimiz bir örnek de, Google'ın video izleme, yükleme ve paylaşma servisi olan YouTube'dur. Youtube üzerinde kullanıcılar kendi videolarını yükleyebilmekte ve diğer kullanıcılar ile bu videoları paylaşabilmektedir. Sitenin kullanımı ve popülerliği kullanıcıların video yüklemesine ve izlemesine bağlı olduğundan Google bu süreç ile ilgili bir teşvik işlemi tanımlamıştır. Google, videoları izleyen kullanıcılara kısa reklamlar da izletme ve bu reklam ücretlerinin bir kısmını asıl video sahipleri ile izlenme oranı doğrultusunda paylaşmaktadır. Böylece kullanıcıları daha çok video yüklemeye teşvik etmektedir.

Teşvik, insanları başarıya ulaştırmak, istenileni elde etmeye güdüleyen önemli bir işlemdir. İnsanların doğası gereği birçok alanda teşvik önemli bir yer tutmaktadır. Çalışma hayatından insan ilişkilerinde, eğitim hayatından teknolojik alanlarda çeşitli sevide teşvik kullanılmaktadır.

3.2 Güven

Güven, iletişimin olduğu her türlü alanda ortaya çıkan bir kavramdır. Güven; korku, çekinme ve kuşku duymadan inanma ve bağlanma duygusudur. Her türlü insan ilişkisinde güven ihtiyacı ortaya çıkmaktadır.

İletişimin olduğu her alanda güven olmazsa olmazdır. İletişimin karşılıklı muhatapları birbirleri arasındaki süreç boyunca karşılıklı güvene ihtiyaç duymaktadır. Karşılıklı iletişimin olduğu her noktada güven gerekmektedir. İki kişinin çok kısa da olsa konuşması boyunca herhangi bir güven olmaz ise, bu konuşma hiçbir önem taşımamaktadır. Güven olmayan bir ortamda kargaşa, anarşi, tereddütler vardır ve ilişkiler sürdürülebilir değildir.

Güven, geçmişten günümüze birçok alanda inceleme konusu olmuştur. Sosyoloji ve psikoloji başta olmak üzere felsefe, ekonomi gibi alanlar kendi alanları ile ilgili güveni açıklamaya çalışmışlardır. Bilgisayarların olduğu bir ortamda mutlaka bilgisayarlar arasında da iletişim bulunmaktadır. Bu

durumda güven konusu bilgisayar biliminin de konusu olmuştur [16]. Bu açıklamalardan sonra güven; güvenecek olanın beklentilerinin, güvenilecek olanın gerçekleştirdikleri ile karşılanması, ve gelecekte güvenilecek olana kuşku ile bakılmaması olarak tanımlanabilir.

3.3 Eşler Arası Ağlarda Teşvik ve Güven Sistemleri

İnsan ilişkilerinde genel olarak güven ortamı kişilerin söyledikleri, yaptıkları işlerin diğer kişiler tarafından değerlendirilmesi ile gerçekleşir. Bilgisayarlar arası güven daha farklı bir yapı gerektirmektedir çünkü bilgisayarlar arası güven kavramında karşımıza farklı sorunlar çıkmaktadır. Karşıdaki kişinin gerçekten iddia edilen kişi olup olmadığının tespiti, karşıdaki kişinin söylediklerinin gerçekten doğru olup olmadığının tespiti bu sorunların en başındadır. Bu aynı sorunlar eşler arası ağlarda da karşımıza çıkmakta ve eşler arası ağlarda güven önemli bir rol oynamaktadır.

Bir eşler arası ağ sisteminde, tüm kullanıcılar iyi niyetli olmayabilir. Bazı eşler sistemde zararlı veya sahte içerikler paylaşarak sistemdeki diğer eşlere zarar vermek isteyebilirler. Bir kötü niyetli eş, istenen içerik yerine başka bir içerik paylaşımında bulunuyorsa sahte içerik paylaşıyordur. Bu durumda iyi niyetli eş zaman ve bant genişliği kaybına uğrayacaktır. Eğer kötü niyetli eş, istenen içeriği modifiye edip zararlı parçalar saklanmış içeriği paylaşıyorsa zararlı içerik paylaşıyordur. Bu durumda iyi niyetli eş zaman ve bant genişliği kaybının yanında, zararlı parçalar nedeniyle daha çok zarara da uğrayabilir. Bu iki temel problemle başa çıkmak ve kötü niyetli kullanıcıları tespit ederek sistemden soyutlamak için eşler arası ağlarda güven sistemleri geliştirilmiştir. Güven sistemleri kötü niyetli eşleri tespit ederek bu eşlerin içerik paylaşmasını engellemektedir.

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 kaynaklarını kullandıktan sonra ağa katkı sağlamayı bırakmaktadır [2]. Bu durum, ağın etkinliğini ciddi ölçüde etkilemekte ve bazı eşlere fazla yük binmesine sebep olmaktadır. Bu nedenle, ağ üzerindeki bütün eşleri sisteme 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 sisteme daha fazla katkı sağlamaya teşvik etmek ve sisteme herhangi bir fayda sağlamadan sistemden yararlanan kullanıcıları engellemek teşvik modellerinin en önemli görevidir.

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. Ortak Malların Trajedisi Kuramı [17], isminden de anlaşılacağı gibi iktisatta kamu malları gibi ortak malların yaşadığı trajediyi anlatmaktadır. Şöyle ki, kamusal mallar herkes tarafından kullanılması 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 tükenebilir. 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 bankının da aynı kişiler tarafından kullanıldığı varsayılsa bile ufak bir tahmin ile park içindeki bankın çok daha kısa sürede işlevini yitireceği ve eskiyeceğini tahmin etmek mümkündür.

P2P sistemlerin gücü, eşlerin gönüllü paylaşımından gelmektedir. P2P sistemlerinde merkezi bir otoritenin olmaması ve gücünün gönüllü paylaşımdan 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 [2]. Örneğin; Gnutella ve Napster üzerinde yapılan araştırmalar göstermiştir ki, bu uygulamaları kullanan kullanıcıların %50'sinin oturum süreleri 1 saatten azdır ve çoğunluğu paylaşım yapmamaktadır [18]. Kullanıcıların kendi karlarını artırma isteğinden dolayı ortaya çıkan problemler arasında en yaygın olanları, bedavacılık (free riding), geçmişi silme (white washing) ve çoklu kimlik tanımlama (sybil attack) problemleridir. Şimdi bu problemleri inceleyelim.

3.3.1 Bedavacılık (*Free Riding)*

Bedavacı kullanıcı sisteme hiçbir katkı yapmadan sistemden yararlanan kullanıcılara denir[2, 19]. 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. Böyle kullanıcılarda "Bir kullanıcı bir şeyi bedava elde edebiliyorsa neden para/kaynak versin ki?" yaklaşımı hakimdir. Bu noktada, kullanıcıları para/katkı vermeye teşvik edecek veya hatta bazen zorlayacak bir sistem olmalıdır.

3.3.2 Geçmişi Silme (*White Washing)*

Bedavacılığı önlemeye yönelik bir yöntem kullanan sistemlerde, bazen bedavacı olan kullanıcılar sürekli olarak sistemden ayrılıp tekrar sisteme katılırlar. Böylece geçmişlerini silerek bedavacılık cezalarından kurtulmaya veya kendilerine avantaj sağlamaya çalışırlar [19, 20]. Özellikle itibara dayalı güven modelleri (*reputation-based trust models*) [6, 21] bu ataklara duyarlıdır. Bu atağın ortaya çıkma nedeni, sistemdeki kimlik alma maliyetinin az olması veya olmaması ve kullanıcıların anonim olarak sisteme katılabilmeleridir. Bu atağı engellemek için kullanıcıların sürekli olarak kimlik değiştirip sahte kimlikle sisteme katılabilmesi çeşitli yöntemler ve cezalarla engellenmeli veya en azından zorlaştırılmalıdır.

3.3.3 Çoklu Kimlik Tanımlama (*Sybil Attack)*

Sybil saldırısında [22], saldırıyı yapan kullanıcı 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 kullanıcı kimliklerini yönetmediği sürece, bu atağın her zaman olma olasılığı vardır.

3.4 Teşvik ve Güven Modelleri İle İlgili Çalışmalar

Son zamanlarda eşler arası ağlarda teşvik ve güven modelleri popülerliği artan konulardandır. Bu nedenle bu konular üzerinde çeşitli araştırmalar bulunmaktadır. Bu kesimde, teşvik modelleri konusunda yapılan araştırmalar incelenmeye çalışılmıştır. Bu çalışma kapsamında yoğunlaşılan güven tabanlı teşvik modelleri üzerine de yapılan çalışmalar

incelenecektir. Bizim hedefimiz genel olarak teşvik ve güven tabanlı teşvik modelleri hakkında mümkün oldukça çok araştırma incelemek olmuştur.

Daha önceki bölümde detaylı olarak anlatıldığı gibi, bir eşler arası ağda sistemden servis alıp sisteme herhangi katkı sağlamayan eşlere bedavacı eş (*free rider*) denilmektedir. Eşler arası ağlarda bedavacı eşler sistem genelinde performans sıkıntılarına neden olmaktadır [2, 23, 24, 25]. Saroui ve diğerlerinin [18] araştırmasına göre Gnutella veya Napster kullanıcılarının %50'sinin oturum süreleri bir saatten daha azdır ve bu kullanıcılar sisteme herhangi bir katkı verme eğiliminde değillerdir. Adar ve Huberman'ın [2] araştırmasına göre Gnutella sistemindeki kullanıcıların %70'i sisteme herhangi bir katkı sağlamamaktadır ve sistemdeki sorguların %50'sine %1'lik bir kullanıcı grubu cevap vermektedir. Bu gibi örnekler bize eşler arası ağlarda teşvik modellerinin kaçınılmaz olduğunu göstermektedir.

Eşler arası ağlarda teşvik modellerini kategorize etmek istediğimizde üç ana kategori oluşturulabilir. Bunlar oyun teorisi kullanan teşvik modelleri, mütekabiliyet tabanlı teşvik modelleri ve mikro ekonomi tabanlı teşvik modelleridir.

3.4.1 Oyun Teosisi Tabanlı Teşvik Modelleri

[26, 27, 28, 29] çalışmaları oyun teorisi [30, 31, 32] tabanlı teşvik modelleri sunmaktadır. Bu teşvik modellerinin genel amacı bir Nash dengesi [33, 34, 35] bulmak ve kurmaktır. Genel olarak bir oyun kurularak, tüm kullanıcıların sisteme katkı sağlayacak şekilde kendi karlarını maksimize edileceği bir denge noktası kurulmaktadır.

Lai ve diğerleri [36], bedavacılık problemini engelleyebilmek ve sistemin yararını artırabilmek için, *evolutionary prisoner's dilamma (EPD)* [37] kullanarak bir teşvik model geliştirmişlerdir. Yazarların geliştirdikleri model ve çalışmalar sonucunda bir teşvik modeli geliştirirken dikkat edilmesi

tavsiye edilen 3 önemli bulgu ortaya koymuşlardır. Bunlar:

- Düğümün (*node*) sadece kendisinin tuttuğu bilgiye dayalı olan teşvik modeller sistem büyüklüğü arttıkça çalışmaz.
- Her düğümün tuttuğu bilgileri birbiri ile paylaşıp bu bilgilere dayalı teşvik modeller sistem büyüklüğünden etkilenmezler ancak bir altyapı gerektirir ve işbirlikçi saldırılardan etkilenirler.
- Yabancı düğümlerin hareketlerini adapte edebilen teşvik sistemler tam bir işbirliği sağlarlar.

Buragohain ve arkaşları [26] geliştirdikleri oyun teorisi tabanlı teşvik modelinde, eşlerin birbirleri ile etkileşimlerini stratejik ve rasyonel oyuncuların olduğu işbirliği olmayan bir oyun (*non-cooperative game*) olarak modellemişlerdir. P2P sistemde her eşin kendi faydasını maksime edeceği düşünülmüş ve her eşin sisteme yaptığı katkı ile sistemden sağladığı fayda kullanılarak bir denge belirlenmiştir. Ma ve diğerleri [28] pareto verimliliğini [38] garanti eden ve doğrusal bir zaman karmaşıklığı olan bir kaynak dağıtım mekanizması geliştirmişlerdir. Bu geliştirilen mekanizma eşlere sisteme katkıda bulunmaları konusunda bir teşvik de sağlamaktadır. Ayrıca yazarlar kaynak isteme ve dağıtma sürecini bir rekabet oyunu (*competition game*) olarak modellemişlerdir ve bu modelin nash dengesini göstermişlerdir. Chen ve arkadaşları [29] ise, tekrarlı oyun (*repeated game*) tabanlı bir teşvik modeli geliştirmişlerdir. Tekrarlı oyunda oyuncu, kendi etkisine göre diğer kullanıcıların gelecekte verebileceği tepkileri değerlendirmelidir.

3.4.2 Mütekabiliyet Tabanlı Teşvik Modelleri

Mütekabiliyeti 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 mütekabiliyet tabanlı olmak üzere ikiye ayrılır. Doğrudan mütekabiliyeti 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 mütekabiliyet, genelde uzun süren etkileşimler içeren uygulamalar için daha uygundur. Örneğin, Bittorrent [39] uygulaması bu modeli kullanır. Deneysel ve analitik çalışmalara göre bu yaklaşım, sistemdeki işbirliğini artırdığını gösterse de, free rider problemini tam olarak çözemez [40].

Dolaylı mütekabiliyet 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*) [6, 21] ile birlikte kullanılır ve doğrudan mütekabiliyet 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 dayanıklı değildir.

James Andreoni [41] 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 sürdürebilir olduğunu söylenir. Benzer şekilde, [19]'in yazarları da bu yaklaşımın benzerini kullanan bir model geliştirmişlerdir.

Bittorrent [39] dünyada çok yaygın kullanılan ve popüler bir eşler arası dosya paylaşım sistemidir [42, 43]. Bittorent'in genel çalışma prensibi, bir dosyayı birçok küçük dosya parçalarına (*chunk*) bölmek ve bu küçük dosya parçalarını aynı anda farklı farklı eşlerden indirilmesini sağlamaktır. Bir

eş sahip olduğu dosya parçalarını farklı eşlere yollarken, aynı anda başka eşlerden başka veya aynı dosyanın parçalarını da indirebilir. Yani eş bir indirme yaparken arka planda kendi sahip olduğu dosyalar ile ilgili parçaları başka eşlere yollar.

Bittorrent'in teşvik modeli bazı durumlarda eşler tarafından alt edilebilir [44]. Birçok eş kendi indirme süreci tamamlandığında oturumlarını sonlandırma eğilimindedir. Bu nedenle eğer bir eşin veri indirme kapasitesi (*download capacity*), diğer eşlerin veri indirme kapasitelerinden yüksek ise bu eş sistemden daha çok yararlanma imkanına sahiptir.

BitTorrent'teki teşvik mekanizması tit-for-tat stratejisine veya mahkumlar çıkmazı modeline dayanan yükleme ile orantılı bir indirme mekanizmasıdır. Tit-for-tat stratejisi, kaynak paylaşımı ile kaynak indirimini dengelese ve zamanla evrensel dengeye ulaşan bir strateji olsa dahi, pratikte yüksek kapasitedeki 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 [39] uygulamasının ana fikri, BitTorrent'teki yükleme 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 mütekabiliyet 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 [44]. BitTyrant'ın bu performansı şöyle açıklanabilir: a)yüksek kapasiteli eşler için azalan marjinal fayda prensibini içerir b)düşük kapasitedeki eşlere sistemden göreli fazla fayda sağlar. Fakat BitTyrant'ın artan performansı bize bir maliyet ile döner. Yeni kullanıcıların uzun ön yükleme süreleriyle karşılaşmaları buna örnek verilebilir.

Credence [45] 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 tanımında, belirtilen içeriğe sahip olmayan her şey olarak tanımlanmıştır. Bu modeli ortaya koyan yazara göre, içeriğin kirli olup olmadığını değerlendirmede en etkin yol, matematiksel ve istatiksel yöntemlere oranla dürüst kullanıcılardır. 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-repudation*) 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, dürüstlüğe teşvik edilir. Sistemin dezavantajı olarak daha önceden uzun süre dürüst olan bir kullanıcı davranışını değiştirip yalan söylerse küçük bir küme için sonuçları etkileyebilir.

3.4.3 Mikro Ekonomi Tabanlı Teşvik Modelleri

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 kullanılmamasını 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.

Wallach ve diğerleri [46], kendi paylaşım yaptığı kadar indirme yapabilmeyi limitleyen adil bir paylaşım sistemi oluşturabilmeyi amaçlamışlardır. Bunun için, sistemdeki tüm kullanıcıların yaptıkları işlemlerin kayıt altına alınması hedeflenmiştir. Bu kayıt işlemi sonucunda bir kullanıcının sisteme verdiği katkı sistemden aldığı katkıdan büyük ise kullanıcının indirme yapmasına izin veren bir model geliştirmişlerdir.

Karma [47], 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 kullanıcı sanal para kazanır. Karma, bir kullanıcının sisteme sağladığı katkıları ve sistemden aldığı yararları takip ederek bedavacılarla savaşır. 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*) [9] 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 deflasyon 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 eşi 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 imzalanmıştır. 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.

Golle ve diğerleri [48], bedavacılık problemi ile başa çıkabilmek için informal bir oyun teorisi modeli kurmuş ve çeşitli *payment modelleri* altında bu kullanıcıların dengesini analiz etmiştir. Yazarların kurdukları modelde kullanıcıların kendi faydalarını maksimize etmek için bencil davranacakları varsayılmış ve buna göre sisteme çeşitli payment modelleri eklenip kullanıcıların davranışlarını analiz edilmiştir. Yani geliştirilen model hem oyun teorisini hem de sanal para şemasını birleştiren bir yaklaşımdır.

Yazarlar geliştirdikleri modelin Napster üzerinde benzetimi yapmış ve modelin başarısını paylaşmışlardır.

[49] araştırmasında Zhao ve arkadaşları, bir itibar (*reputation*) sisteminde doğru geribildirimler bırakılması için bir teşvik modeli geliştirmişlerdir. Bir itibar sisteminin gücü geribildirimlerden gelmektedir. Bu nedenle geribildirimlerin doğru bir şekilde bildirilmesi gerekmektedir. Zhao ve arkadaşları, ücret kullanan mikro ekonomi tabanlı bir teşvik modeli kullanarak kullanıcıların doğru bir şekilde geribildirimde bulunmaları sağlanmıştır.

Güven modelleri genellikle kullanıcıların diğer kullanıcılara verdikleri değerlendirmeler üzerine kurulan modellerdir. Her bir kullanıcının kendi itibarı olmaktadır. Diğer kullanıcılar bu itibarları ve diğer kullanıcıların tavsiyelerini değerlendirerek güven hesaplamaktadırlar. [50]'de yazarlar tavsiye tabanlı global bir güven modeli kurmuşlardır. Yazarların yaptığı benzetim sonuçlarına göre geliştirdikleri itibar tabanlı güven modeli mevcut modellere göre çoklu kimlik tanımlama gibi saldırganlarda güvenlik yönünden daha başarılı sonuçlar vermiştir. [51] çalışmasında ise yazarlar eşler arası ağlarda e-ticaret sistemleri için itibar tabanlı bir güven modeli sunmuşlardır. Sundukları modelde bir kullanıcının hem yerel hem de global itibar değeri olmak üzere iki itibar puanı olmaktadır. Yerel itibar değeri direkt olarak seçilecek kullanıcı ile yapılan geçmiş etkileşimlerden kullanıcının kendisinin verdiği itibar değeri iken, global itibar değeri tüm kullanıcıların seçilecek kullanıcı hakkında verdiği itibar değeridir. İkili itibar değerlendirme sistemine model ile yazarlar eşler arası ağlarda e-ticaret sistemlerinde başarılı sonuçlar almışlardır.

Liang ve arkadaşları [52] bir güven modelinde kısa vadeli güvenirlik kavramında risk kavramını ele alan ilk modeldir. Yazarların PET ismini verdikleri modelleri iki parçadan oluşmaktadır. Bunlardan ilki itibar değerlendirme iken ikincisi risk değerlendirmedir. Modele göre

itibar değerlendirme, uzun vadeli davranışların değerlendirmesidir ve risk değerlendirmesi kısa vadeli davranışların değerlendirmesidir ve kullanıcıların sonradan davranışlarını değiştirmesi durumunu ele almaktadır. Benzer şekilde [53] çalışmasında yazarlar, itibarları zaman çerçevesi içerisinde değerlendirerek kısa vadeli güven ve uzun vadeli güven değerleri hesaplamış, dinamik bir güven modeli geliştirmişlerdir.

Global güven modelleri genel olarak en yüksek güven değerine sahip, kullanıcının en güvenilir olduğu varsayımı üzerine kurgulanır ve her bir kullanıcının global bir güven değeri bulunmaktadır. [54] çalışmasında bir kullanıcının başka kullanıcılar tarafından verilmiş itibar değeri benzerliğine göre ağırlıklandırılarak (*similarity-weighted*) hesaplanmıştır. Bu yöntem yardımıyla işbirliği içerisinde bulunan saldırganların global güven modellerinin varsayımını yıkabileceği ve geliştirilen modelin bu durumu ele alabileceği gösterilmiştir. [55] çalışması ise geçersiz, doğru olmayan tavsiyeler problemi ile başa çıkmak için bir model sunmuştur. Modelde, tavsiyeler değerlendirilmeden önce bir filtreden geçirilerek, yanlış *noisy* tavsiyeler elenir. Ayrıca yazarlar geri bildirime dayalı olası *feedback-based probabilistic* bir tavsiye arama algoritması da sunmuşlardır.

Eşler arası ağlarda güven ve teşvik metriklerinin saklanması ve gerektiğinde bu metriklere ulaşmak da ayrı bir problemdir. Her bir eş diğer eşler hakkında geçmiş bilgilerini kendi saklayabilir ve bir sorgu geldiğinde cevaplayabilir. Ancak bu durum ağda *flooding* olarak bilinen problemi ortaya çıkarmakta ve ağın etkinliğini düşürmektedir. Ayrıca böyle bir durumda kötü niyetli eşler çeşitli saldırılar da yapabilmektedir [56]. Bu nedenlerden dolayı birçok model metriklere erişimde önceki bölümde bahsettiğimiz DHT prokolünü kullanmıştır.

Literatür araştırmasında, birçok teşvik modelinin oyun teorisi tabanlı olduğu fark edilmiştir. Bu modellerde genel olarak tüm eşler kendi karlarını maksimize etmeye çalışan rasyonel kullanıcı olarak kabul edilmiştir ve bu

kapsamda bir oyun kurulmuştur. Ancak literatürde güven modelini ve metriklerini kullanan herhangi bir teşvik modeline rastlanmamıştır. Sadece [57] araştırmasında yazarlar güven tabanlı bir teşvik modeli için bir survey sunmuşlardır. Bizim amacımız ise bu eksikliği tamamlayacak şekilde güven modeli tabanlı ve güven metrikleri kullanan bir teşvik modeli oluşturmak olmuştur.

4 MODEL VE YÖNTEM

Bu tez kapsamında yapılan çalışmalarda eşler arası sistemlerdeki güven modeli tabanlı bir teşvik modelinin geliştirilmesi amaçlanmıştır. Bu kapsamda oluşturulan modelin varsayımları, geliştirilme süreçleri ve modülleri anlatılacaktır.

4.1 Varsayımlar

Modelin anlatımına geçmeden önce modelin kabul ettiği bazı varsayımlardan bahsetmek gerekmektedir. Bu kabuller modelin ve benzetimin daha etkin bir şekilde gerçekleştiriminin sağlanması için yapılmıştır.

Sistemin ilk kabulü sistemde tutulan güven ve teşvik ile ilgili metriklerin saklanması ve erişilmesi ile ilgilidir. Sistemdeki eşlerin güven ve itibar metriklerinin saklanmasının ve erişiminin DHT ile sağlandığı varsayılmıştır. Böylece eşlerin sistemdeki tüm bilgisayarlar üzerinde sorgu yaparak, ağ trafiğini artırmadan metriklere erişimi ve metriklerin saklanması sağlanmıştır.

Sistemin ikinci ve son kabulü ise eşlerin ilk indirme işlemleri ile ilgilidir. Kabule göre her bir eş sistem genelinde yapacakları ilk indirme işlemlerinde herhangi bir sınırlandırma uygulanmamaktadır ve eşler ilk indirmede istedikleri herhangi bir dosyayı indirebilmektedirler.

4.2 Model

Eşler arası sistemlerde teşvik modeli kurulması, çözülmesi zor bir problemdir. Daha önceki birçok model oyun teorisi tabanlı olup sistemdeki kullanıcıların davranışları odaklı bir oyun kurup bir denge hedeflemekte ve

bu yöntem ile bir eşitlik sağlamayı amaçlanmıştır. Ayrıca var olan bazı modeller ise mikro ekonomi tabanlı bir ödeme sistemi ile kullanıcıların kazandığı kadar harcama ile veya tasarımsal olarak bir eşitlik sağlamayı hedeflemişlerdir. Ancak var olan modellerin çok azı güven modellerini taban alan bir yapı kurmamıştır.

Bu tez çalışmasında önerilen model, aşamalar halinde geliştirilmiş olup, üç aşamalı olarak tasarlanmıştır. Bu aşamaların her birinde bir önceki aşamaya göre model daha detaylı problemleri çözmüş veya dezavantajlarını indirgemiştir.

4.2.1 Paylaşım Oranı Modeli

Modelin ilk aşaması Paylaşım Oranı Modeli adı verilen modeldir. Bu modelin amacı her bir eşin sisteme yaptığı katkı ile sistemden alınan servislerin kayıt altına alınarak; bu kayıtlar doğrultusunda bir eşitlik sağlamaktır.

Çizelge 1: Metrikler

Metrik	**Açıklama**
Toplam İndirme (*download*)	Bir eş tarafından sistem başlangıcından beri yapılan toplam indirme miktarı (byte olarak)
Toplam Gönderme (*upload*)	Bir eş tarafından sistem başlangıcından beri yapılan toplam gönderme miktarı (byte olarak)
Toplam İndirme Sayısı	Bir eş tarafından sistem başlangıcından beri yapılan toplam indirme sayısı
Toplam Gönderme Sayısı	Bir eş tarafından sistem başlangıcından beri yapılan toplam gönderme sayısı

Bu aşamada sistemdeki her bir eşin yaptığı indirme ve gönderme verileri DHT üzerinde saklanır. Bir eş başka bir eşten bir veri indirmek istediğinde, indirme işlemi bittiği anda indirme yapan eş ile ilgili DHT üzerindeki toplam indirme metriğine verinin boyutu eklenmektedir. Aynı şekilde gönderen eş ile ilgili DHT üzerindeki toplam gönderme metriğine verinin boyutu

eklenmektedir. Yani bu işlemler sonucunda her bir eşin toplam gönderme miktarı, toplam indirme miktarı, toplam indirme sayısı, toplam gönderme sayısı metrikleri anlık olarak erişilmekte ve güncellenmektedir.

Tutulan metrikler yardımıyla model bir teşvik sistemi sağlamayı amaçlamıştır. Modele göre sistemde bir eşik oranı belirlenmektedir. Bu eşik oranı (l) aşağıda 4.1 matematiksel olarak gösterildiği gibi sistemdeki tüm eşlerin verilerinden elde edilmektedir. Sistemdeki her bir eşin maksimum veri gönderme kapasitelerinin (u_j) toplamı, sistemdeki her bir eşin maksimum veri indirme kapasitelerinin (d_j) toplamına oranlanarak eşik oran değeri hesaplanmaktadır.

$$l = \frac{\sum_{j=1}^{n} u_j}{\sum_{j=1}^{n} d_j} \tag{4.1}$$

Sistemde bir eş bir başka bir eşten indirme isteğinde bulunduğunda, indirme yapacak eşin güncel metrikleri ile paylaşım oranı (r, *instant ratio*) hesaplanmaktadır. Bu hesaplama matematiksel olarak aşağıda 4.2 ile gösterilmiştir. Buna göre indirme yapacak eşin toplam gönderme miktarı (u_j), toplam indirme miktarı (d_j) ile indirilecek içeriğin boyutunun (f) toplamına oranlanması ile bir eşin paylaşım oranı hesaplanmaktadır. Hesaplanan bu iki oran değeri ile bir eş indirme isteğinde bulunduğunda eşin paylaşım oranı, eşik oran değerinden (l) büyük ise eşe indirme izni verilmekte, eşik değerinden küçük ise indirme izni verilmemektedir. Bu anlatılan metnin matematiksel ifadesi aşağıda gösterilmiştir.

$$r = \frac{u_j}{d_j + f} \geq l \tag{4.2}$$

Geliştirilen ilk aşamada sadece eşlerin toplam indirme ve gönderilme

miktarlarına göre basit bir teşvik modeli kurulmuştur. Bu ilk aşama bize belli bir seviyede teşvik sağladığı halde, sadece bazı durumları engelleyebilmekte bazı durumlarda ise etkisiz kalmaktadır. Benzetim bölümünde detaylı olarak sonuçlarının inceleneceği bu aşamada bireysel davranış gösterip içerik paylaşmayan eşler (*free rider*) sistemde engellenebilmektedir. Ancak bireysel davranış yerine iş birlikçi davranışta bulunan eşler için modelin yeterli olmayacağı açıktır. Sistem içerisinde işbirlikçi kötü niyetli eşler kendi aralarında gönderme ve alma işlemi göstererek teşvik modelini kandırabilirler.

4.2.2 Güven Tabanlı Model

Tek başına oran tabanlı bir limitleme yeterli değildir. Kötü niyetli ve iş birlik yapan eşler kolaylıkla böyle bir sistemi alt edebilirler. Örneğin çoklu kimlik tanımlama atağı (*sybil attack [22]*) yapan bir eş başka eşlere ihtiyaç dahi duymadan kolaylıkla böyle bir sistemi alt edebilir veya işbirliği içinde olan kötü niyetli iki eş sürekli olarak sadece birbirlerine dosya göndererek kendi paylaşım oranlarını yükseltebilirler. Bu nedenle geliştirdiğimiz modelin ikinci aşaması güven tabanlı modeldir.

Modelin çalışma prensibine geçmeden önce, güven modellerinden bahsetmek gerekmektedir. Güven modelleri kullanıcıların gerçekten doğru ve herhangi bir zararlı parça içermeyen paylaşımlar yapmasını sağlayan modellerdir. Güven modellerinde genel olarak, kullanıcılar hizmet aldıkları eşlere aldıkları hizmet karşılığında puanlar verirler ve eşlerin bu puanlarına göre en güvenilir ve en uygun olan eşi hizmet almak için seçmeye çalışırlar. Güven modelleri yardımı ile sahte veya zararlı içerik paylaşan eşler düşük güven puanları aldıklarından hizmet almak için seçilmezler.

Güven modelleri kullanıcıların dürüstlüğü ile ilgili metrikler toplarlar. Bu metrikler hizmet alan eşler tarafından hizmet alınan eşe verilir. Böylece bir eşin dürüstlüğü geçmişte verdiği hizmetlerin kalitesi ile ölçülür. Fakat

metriklerin de bir yaşlanma ölçüsü olmalıdır. Çünkü belirli bir süre doğru ve güvenilir içerik paylaşan bir eş, kötü niyetli paylaşımlar yapmaya başladığında itibarını çok eski hizmetlerinden almamalıdır.

Teşvik modeli için bir güven modelinin seçilmesi teşvik modeline güven modelinin topladığı metrikleri kullanma özgürlüğünü sağlayabilir. Basit olarak bir eşin hizmet alabilmesi için, o eşin güven metriklerine bakılarak güvenilir olup olmadığına göre izin verilebilir. Böylece eşlere paylaşımda bulunarak hem güven kazanması hem de paylaşımda bulunması teşviki sağlanabilir.

Güven Tabanlı Model adını verdiğimiz modelimiz de bu prensibe dayanmaktadır. Bu çalışmaya temel olarak alınan güven modelinde [58] eşlerin birbiri ile daha önceden bir işlem yapıp yapmamasına göre komşuluk tanımlanmıştır. Buna göre eğer iki eş daha önceden bir indirme-gönderme işlemi yapmış ise bu eşler komşu eşlerdir. Ayrıca her bir eşin kendi sağladığı servisin güven değerini belirten bir servis güven değeri mevcuttur. Bir komşu eşin servis güven değeri, bu komşu eş ile yapılan geçmiş deneyimlerin ortalaması olarak hesaplanırken, komşu olmayan bir eşin servis güven değeri hesaplanacak ise, bu eş hakkında komşulardan tavsiye istenir ve gelen tavsiyelere göre hesaplanır.

Güven Tabanlı Modelde eğer bir eş bir indirme yapmak istiyor ise, model öncelikle birinci aşamadaki gibi indirme yapacak eşin toplam gönderme miktarı, toplam indirme miktarı ile indirilecek içeriğin boyutunun toplamına oranlanması ile eşin paylaşım oranı hesaplanmaktadır. Bu oran ile eşik oran değeri karşılaştırılmakta ve eşin paylaşım oranı eşit oran değerinden büyük ise; ikinci aşamada eşin güven metriklerine özgü kontrol yapılmaktadır. Buna göre ilk olarak indirme yapacak eşin ortalama servis güven değeri hesaplanmaktadır. İndirme yapacak eşin servis güven değeri hesaplandıktan sonra model hizmet sağlayacak eşin komşularının ortalama güven değerinin standart sapmasını hesaplamaktadır. Bu iki değer ile model

bir güven eşik değeri belirlemektedir. Hesaplanan indirme yapacak eşin servis güven değerinden, hizmet sağlayacak eşin komşularının ortalama güven değerinin standart sapması çıkarılarak eşik güven değeri elde edilmektedir. Güven eşik değerinin hesaplanmasından sonra model indirme yapacak eşin, hizmet sağlayan eş ile komşu olup olmadığını kontrol etmektedir. Eğer eşler komşu ise; model hizmet sağlayacak eşin, indirme yapacak eş ile herhangi bir kötü bir geçmiş yaşayıp yaşamadığını yani indirme yapacak eşin önceden hizmet sağlayan eşe sahte veya zararlı içerik yollayıp yollamadığını kontrol etmektedir. Eşler kötü bir geçmiş yaşamışlar ise model indirme isteğini anında reddeder, eğer yaşamamışlar ise; indirme yapacak eşin servis güven değeri güven eşik değeri ile karşılaştırılır. Karşılaştırma sonucunda eğer indirme yapacak eşin servis güven değeri güven eşik değerinden büyük ise indirmeye izin verilir, değil ise indirme reddedilir. Eğer eşler komşu değiller ise, indirme yapacak eşin güven değerinin hesaplanabilmesi için ilk olarak komşulardan indirme yapacak eş hakkında tavsiyeler ve ün toplanır. Bu toplanan değerler ile indime yapacak eşin güven değeri hesaplanır ve hesaplanan değer güven eşik değerinden büyükse indirmeye izin verilir. Tam tersi bir durumda yani hesaplanan değer güven eşik değerinden küçükse indirme reddedilir. Anlatılan bu kontrol mekanizması Algoritma 1 olarak aşağıda ifade edilmiştir.

Ayrıca Güven Tabanlı Modelin matematiksel ifadesi aşağıda gösterilmiştir. Sistemde ilk olarak bir ortalama güven değeri ($avest$) hesaplanır (eşitlik 4.3). Bu değer indirme yapacak eşin komşularının (n) bu eş hakkında verdikleri güven değerlerinin (st) ortalaması alınarak hesaplanır. Ardından sistemdeki indirme yapacak eşin komşularının bu eş hakkında verdikleri güven değerlerinin standart sapması ($stddevst$) hesaplanarak, eşik güven değeri (th) hesaplanır (eşitlik 4.4, 4.5). Bir eş indirme yapmak istediğinde, gönderme yapacak eşin hesapladığı güven değeri (st), hesaplanan eşik güven değerinden (th) büyük ve indirme yapacak eşin paylaşım oranı ($u_j/d_j + f$) eşik orandan (l) büyük ise eşin indirme yapmasına izin verilirken aksi durumlarda eşin indirme isteği reddediir. (eşitlik 4.6)

Algoritma 1 Güven Tabanlı Model Çalışma Adımları

```
güven eşik değerini hesapla
if indirme yapacak eş komşuysa then
  if indirme yapacak eş ile kötü geçmiş yaşandı mı then
    isteği reddet
  else
    indirme yapacak eşin güven değerini hesapla
    indirme yapacak eşin paylaşım oranını hesapla
    if güven değeri, güven eşik değerinden büyük ve paylaşım oranı eşik
    orandan büyükse then
      isteği onayla
    else
      isteği reddet
    end if
  end if
else
  indirme yapacak eş hakkında komşulardan tavsiye topla
  indirme yapacak eş hakkında komşulardan ün hesapla
  indirme yapacak eşin güven değerini hesapla
  indirme yapacak eşin paylaşım oranını hesapla
  if güven değeri, güven eşik değerinden büyük ve paylaşım oranı eşik
  orandan büyükse then
    isteği onayla
  else
    isteği reddet
  end if
end if
```

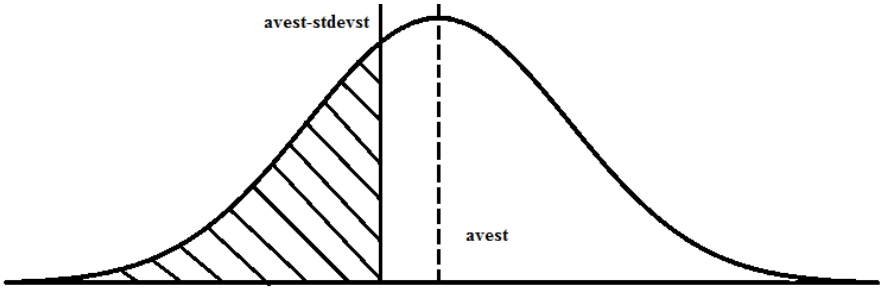
$$avest = \frac{\sum_{j=1}^{n} st_j}{n} \tag{4.3}$$

$$stdevst = \frac{\sum_{j=1}^{n} (st_j - avest)^2}{n} \tag{4.4}$$

$$\begin{aligned} th &= avest - stdevst \\ &= \frac{\sum_{j=1}^{n} st_j - (st_j - avest)^2}{n} \end{aligned} \tag{4.5}$$

$$t_j = \begin{cases} st \geq th \quad ve \quad u_j/d_j + f \geq l, \quad izin\ ver \\ st \geq th \quad ve \quad u_j/d_j + f < l, \quad reddet \\ st < th \quad ve \quad u_j/d_j + f \geq l, \quad reddet \\ st < th \quad ve \quad u_j/d_j + f < l, \quad reddet \end{cases} \tag{4.6}$$

Aşağıdaki Şekil 4 bir eşin komşularının servis güven değerinin normal dağılım varsayıldığı durumu göstermektedir. Buna göre eşin komşularının ortalama güven değeri ve güven eşik değeri şekil üzerinde gösterilmiştir. Güven eşik değeri hesaplamasında eşin komşularının ortalama güven değerinden, standart sapma çıkarılarak indirmeye izin verilecek sınır düşürülmüştür. Böylece ortalamaya göre daha çok eşe izin verilerek iyi niyetli eşlerin sınırlamadan daha az etkilenmesi amaçlanmıştır. Şekildeki taralı alanda bulunan eşler model tarafından indirme yapmaya izin verilmeyen alanı göstermektedir. Normal dağılım gösteren bir sistemde bu



Şekil 4: Servis Güven Değerinin Normal Dağılımı

eşik değeri, eşlerin $\Phi(-0.5) = 0.3185$ [58] kadarını sınırlamaktadır.

Güven metriklerinin kullanımı ile geliştirilen Güven Tabanlı Model ile birlikte, iş birliği içinde bulunan kötü niyetli eşlerin dahi engellenebilmesi beklenmektedir. Güven modeli ile eşlere doğru ve zararlı parçalar içermeyen paylaşım yaparak kendilerini kanıtlama zorunluluğu getirilmiştir. Eğer bir eş hiç bir eşe paylaşımda bulunmaz ise, diğer tüm eşlere karşı yabancı durumda olacak ve indirme yapmasına izin verilmeyecektir. Güven Tabanlı Model ile bedavacılık (*free riding*) ve çoklu kimlik tanımlama (*sybil attack*) problemlerinin çözülmesi beklenmektedir.

4.2.3 Güven Tabanlı Uyarlanabilir Model

Güven Tabanlı Model ile bireysel ve işbirlikçi kötü niyetli eşler engellenebilmiştir. Ancak model ile birlikte iyi niyetli kullanıcılar da sistemin başlangıcında etkilenmektedirler. Çünkü teşvik modeli ile birlikte sisteme dahil olan tüm eşler başlangıç aşamasında kendilerini kanıtlamak zorundadırlar. Bu nedenle eşler iyi niyetli olsalar dahi sistemin başlangıcında indirme yönünden sınırlamalar ile karşılaşmaktadırlar.

Bu noktada eşlere uygulanan eşik oranın sabit bir değer olmasındansa eşin davranışına göre değer alan bir eşik oranının uygulanması prensibine dayanan modele Güven Tabanlı Uyarlanabilir Model adı verilmiştir. Bu model ile birlikte eşlere sistemin başından sonuna kadar bir sabit oran

uygulanması yerine eşlerin sistemden hizmet almasına veya sisteme hizmet sağlamasına göre dinamik bir eşik oranı uygulanır. Böylelikle iyi niyetli kullanıcıların çok daha hızlı bir şekilde kendilerini modele kanıtlaması ve sınırlamalardan daha az etkilenmesi hedeflenmiştir.

Modele göre başlangıçta her eş Eşitlik 4.1 ile hesaplanan bir eşik oranına göre değerlendirilir. Eşlerin gönderme işlemlerine veya indirme isteklerinin reddedilmesine göre bu sabit oran değiştirilir. Güven tabanlı modelde anlatılan Algoritma 1'e göre eşe indirme yapmasına izin verilir veya eş reddedilir. Eğer bir eş herhangi bir şekilde bir başka eşten reddedilmeden beş kere arka arkaya başarılı indirme işlemi yapabilir ise; model bu eşin daha önceden sisteme katkı sağladığını anlayarak, bu eşin eşik oranını 0,1 azaltarak bu eşi ödüllendirir. Aynı şekilde eğer bir eş arka arkaya beş kere indirme isteklerinden ret alır ise, model bu eşin sisteme katkı yapmadan sistemden fayda sağlamaya çalıştığını anlayarak eşik oranını 0,1 artırarak bu eşi cezalandırır. Modeldeki bu değerler deneysel olarak belirlenmiştir. Sistemde bir eşin eşik oranı hiç bir zaman 0,1'in altında, 0,5'in de üstünde olamaz. Aşağıdaki Algoritma 2 anlatılan yapının detaylı algoritmasını göstermektedir

Bu geliştirilen son model ile birlikte iyi niyetli kullanıcılar sistemden daha kolay bir şekilde yararlanacak şekilde ödüllendirilir iken; kötü niyetli kullanıcılar daha fazla şekilde cezalandırılmaktadır. Böylece iyi niyetli eşlerin daha kolay ve daha fazla indirme yapabilmesi beklenirken; kötü niyetli kullanıcıların daha da az indirme yapabilmesi beklenmektedir.

Algoritma 2 Uyarlanabilir Model Çalışma Adımları

```
if eş indirme yapmak için izinli mi then
  izin verilme sayısını bir artır
  reddedilme sayısını sıfırla
  if izin verilme sayısı beşe eşit mi then
    if eşik değeri minimum değerden büyük mü then
      eşik değerini 0,1 azalt
    end if
    izin verilme sayısını sıfırla
  end if
else
  izin verilme sayısını sıfırla
  reddedilme sayısını bir artır
  if reddedilme sayısı beşe eşit mi then
    if eşik değeri maksimumdan küçük mü then
      eşik değerini 0,1 artır
    end if
    reddedilme sayısını sıfırla
  end if
end if
```

5 DENEYLER VE ÇALIŞMALAR

Geliştirdiğimiz modelleri test edebilmek ve modellerin başarısını ölçebilmek için gerçeğe yakın bir benzetim gerekmektedir. Benzetim bu ihtiyaçları karşılayabilmeli ve kolaylıkla kendi modelimizi gerçekleştirebildiğimiz özelliklere sahip olmalıdır. Bu nedenle benzetim Can ve Bhargava [58] çalışması temel alınarak oluşturulmuştur. Temel alınan güven modelinin de aynı çalışmadan alınması benzetimin gerçeğe yakın olması ve kolaylıkla geliştirmeler yapılabilmesi bu benzetimin seçimi için etkin roller oynamıştır. Temel alınan çalışmanın [58] yaklaşık %40 oranında değiştirilmesi ve geliştirilen teşvik modellerinin eklenmesi ile kullanılan benzetim elde edilmiştir. Benzetim tamamen JAVA programlama dili kullanılarak geliştirilmiştir.

Benzetim, mümkün olduğunca gerçek hayattaki eşler arası ağ uygulamasına yakın olarak geliştirilmeye çalışılmıştır. Benzetimde tüm kullanıcılar (*eşler*) çeşitli dosyalar indirmekte ve indirme isteklerine

cevaplar vermektedirler. Benzetimdeki kullanıcılar iki çeşittir. Kullanıcılar davranışlarına göre iyi niyetli ve kötü niyetli olarak ayrılmaktadır. İyi niyeti kullanıcılar sisteme dahil olduktan sonra teşvik modelinin izin verdiği ölçüde dosya indirme isteklerinde bulunmakta ve gelen dosya gönderme isteklerine cevap vermektedirler. Herhangi zararlı veya kandırıcı işlemler yapmamaktadırlar. Kötü niyetli kullanıcılar ise kendi içinde davranışlarına göre çeşitli türlere ayrılmaktadırlar. Kötü niyetli kullanıcılar mümkün olduğunca teşvik sistemini kandırmaya çalışmakta ve içerik paylaşmadan veya çok az paylaşarak yine mümkün olduğunca çok dosya indirmeye çalışmaktadırlar.

Benzetim başlangıcında belirli sayıda kullanıcı bulunmaktadır ve bu kullanıcıların her zaman %20'si kötü niyetli kullanıcılar iken kalanları iyi niyetli kullanıcılardır. Sistemde başlangıçta her kullanıcı birbiri ile yabancıdır. Yani birbirleri ile herhangi bir geçmiş deneyime sahip değillerdir. Sistemde iki kullanıcı arasında dosya indirme-gönderme işlemi "etkileşim (*transaction*)" olarak adlandırılmaktadır. Kullanıcılar her bir etkileşim sonrası alınan dosyanın istenilen dosya olması ve herhangi zararlı içerik içermemesine göre birbirleri ile komşu olmaktadırlar. İndirilen dosya istenilen dosya değilse veya zararlı bir içerik içeriyorsa, indirme yapan kullanıcı dosyayı gönderen kullanıcıyı kötü geçmiş listesine ekler ve bu kullanıcı ile bir daha herhangi bir etkileşimde bulunmaz. Benzetimde kullanıcılar gerçek hayatta olduğu gibi çevrim içi veya çevrim dışı olabilmektedir. Herhangi bir kullanıcı çevrim içi olduğu süre boyunca aynı anda belli sayıda etkileşimde bulunabilmektedir Ayrıca dosya gönderimi yapan kullanıcının çevrim dışı olma süreleri bu kullanıcının güven değerini etkilemektedir ve eğer dosya gönderen kullanıcı belirli süreden sürekli çevrim dışı ise etkileşim iptal edilmekte ve bu kullanıcı o etkileşimden 0 değerini almaktadır.

Kullanıcılar bir dosya indirmek istediğinde bu dosyayı indirebileceği kullanıcıları bulmakta ve eğer bu kullanıcılar içerisinde komşu kullanıcı varsa

en yüksek güven değerine sahip, aynı anda ele alabileceği maksimum etkileşim sayısına ulaşmamış komşu seçilir. Eğer kullanıcılar içerisinde herhangi bir komşu yoksa yabancı kullanıcılar hakkında komşulardan tavsiyeler istenir. Elde edilen tavsiyelere göre bu yabancıların güven değerleri hesaplanır ve yine en yüksek güven değerine sahip, aynı anda ele alabileceği maksimum etkileşim sayısına ulaşmamış kullanıcı seçilir. Kötü niyetli kullanıcılar yanıltıcı tavsiyeler verebilmektedir.

Benzetimin gerçek eşler arası sisteme benzetilmesi için kullanıcı davranışları gerçeğe yakın modellenmeye çalışılmıştır. Her bir kullanıcının benzetimin başında Çizelge 2(d)'ye göre belirlenen indirme ve gönderme bant genişlikleri bulunmaktadır. Ayrıca her bir dosyanın boyutu da Çizelge 2(a)'ya göre rastgele belirlenmektedir. Bu sayede bir kullanıcı bir dosya indirmek istediğinde dosyanın boyutu, indirme yapacak kullanıcının indirme bant genişliği ve gönderme yapacak kullanıcının gönderme bant genişliği etki etmektedir ve bu parametrelere göre dosyanın indirilme süresi belirlenmektedir.

Benzetimde gerçek bir eşler arası sisteme yaklaşabilmek için çeşitli farklı parametreler bulunmaktadır. Bu parametreler birçok gerçek çalışmaların sonuçlarına göre belirlenerek gerçeklik artırılmaya çalışılmıştır [59, 18, 60, 61]. Çizelge 2 kullanılan parametreleri göstermektedir. Dosya boyutu dağılımı benzetimde her bir dosya boyutunun hangi aralıkta ne oranlarda oluşturulduğunu göstermektedir. Tüm dosyalar bu oranlar dahilinde ve aralıklarının içerisinde yer alacak şekilde rastgele yaratılmaktadır. Başlangıç dosya sahip olma dağılımı, her bir kullanıcının benzetim başlangıcında ne kadar sayıda dosyaya sahip olduğunu aralıklara göre oransal dağılımını göstermektedir. Benzetim başlangıcında tüm kullanıcıların sahip olduğu dosya sayısı bu oranlara göre aralık içiresinde olacak şekilde rastgele belirlenmektedir. Paylaşılan dosya dağılımı benzetim başlangıcında her bir kullanıcının ne kadar dosya paylaştığının aralıklarının oransal dağılımını göstermektedir. Benzetim başlangıçta tüm kullanıcıların en az bir

Çizelge 2: Benzetimde Kullanıcı ve Kaynak Girdilerini Oluşturan Temel Parametreler

(a) Dosya Boyutu Dağılımı

Dosya Boyutu (kb)	Oran
100 - 1000	0.10
1001 - 10000	0.75
10001 - 100000	0.10
100001 - 1000000	0.05

(b) Başlangıç Dosya Sahip Olma Dağılımı

# Dosya	Oran
1 - 5	0.60
6 - 10	0.20
11 - 20	0.15
21 - 40	0.05

(c) Paylaşılan Dosya Dağılımı

# Paylaşılan Dosya	Oran
0 - 0	0.0
1 - 20	0.38
21 - 100	0.42
101 - 200	0.15
201 - 400	0.05

(d) Bant genişliği Dağılımı

İndirme-Yükleme Bant genişliği (kbps)	Oran
128 - 64	0.10
512 - 128	0.10
1024 - 256	0.40
3036 - 768	0.20
10240 - 5120	0.15
102400 - 10240	0.05

(e) Çevirimiçi Periyot Dağılımı

Çevirim içi (Dk)	Oran
61 - 120	0.30
121 - 240	0.50
241 - 360	0.10
361 - 600	0.05
601 - 720	0.05

(f) İndirme Oturumu İçin Bekleme Periyodu

Dosya Boyutu (kb)	Mak. Bekleme Periyot
100 - 1000	1
1000 - 10000	3
10000 - 100000	10
100000 - 1000000	100

dosya paylaşacakları şekilde ayarlanmıştır. Bant genişliği dağılımı her bir kullanıcının sahip olduğu indirme ve gönderme bant genişliklerinin olabileceği aralıkların dağılımını göstermektedir. Buna göre her bir kullanıcının indirme ve gönderme bant genişlikleri Çizelge 2(d)'ye göre kendi aralıkları içerisinde rastgele belirlenmektedir. Çevrim içi periyot dağılımı her bir kullanıcının dakika olarak çevrim içi sürelerini göstermektedir. Son olarak indirme oturumu için bekleme periyodu, indirme yapacak kullanıcıların gönderme yapacak kullanıcıyı indirilecek dosya boyuta göre kaç periyot bekleyeceğini göstermektedir.

Kullanıcıların birbirleri arasında yaptığı etkileşimlerin sonucunda iki değer hesaplanmaktadır ve bu değerler güven hesaplanmasında kullanılmaktadır.

Bunlardan ilki “memnuniyet” değeridir. Bu değer kullanıcının etkileşimden ne kadar memnun kaldığına göre değer almaktadır. Memnuniyet değeri, etkileşimde gerçekleşen ortalama bant genişliği (*AveBw*), etkileşimin başında kararlaştırılmış bant genişliği (*AgrBw*) ve kullanıcıların işlem sırasındaki çevirim içi (*OnP*) ve çevirim dışı (*OffP*) zamanlarını dikkate almaktadır. Memnuniyet [58] çalışmasında olduğu gibi aşağıdaki formüle göre hesaplanmaktadır:

$$\textbf{Memnuniyet} = \begin{cases} (\frac{AveBw}{AgrBw} + \frac{OnP}{OnP+OffP})/2 & if\ AveBw < AgrBw, \\ (1 + \frac{OnP}{OnP+OffP})/2 & otherwise \end{cases} \tag{5.1}$$

Etkileşimin diğer bir özelliği ise etkileşim sonucunda hesaplanan *Ağırlık* değeridir. Bu değer yapılan dosya indirme işlemine göre, dosya boyutu (*size*) ve kullanıcı sayısı (*uploaders, UploaderMax*) ile ilişkilidir. Ağırlık değeri [58] çalışmasında olduğu gibi aşağıdaki formüle göre hesaplanmaktadır:

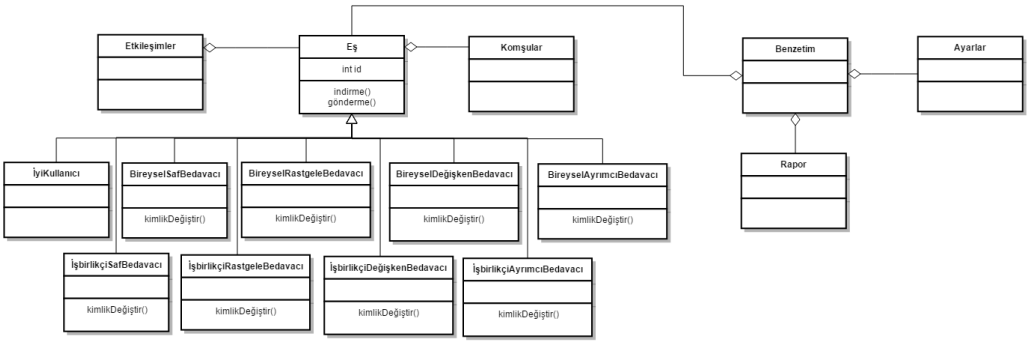
$$\textbf{Ağırlık} = \begin{cases} (\frac{size}{100MB} + \frac{\#Uploaders}{Uploader_{max}})/2 & if\ size < 100MB, \\ (1 + \frac{\#Uploaders}{Uploader_{max}})/2 & otherwise \end{cases} \tag{5.2}$$

Benzetimde her bir kullanıcı, indirme yapmak istediğinde uygulanan teşvik modeline göre indirme yapabilmektedir. Aynı parametrik değerlere sahip kullanıcılar ve dosyalar ile farklı teşvik modellerin benzetimi yapılmıştır. Böylece teşvik modellerinin birbirleri ile karşılaştırılması sağlanmaktadır. Bir kullanıcı indirme yapmak isteğinde, gönderme yapacak kullanıcıyı seçtikten sonra teşvik modeli devreye girmekte ve uygulanan modele göre indirme yapacak eşe izin vermekte veya reddetmektedir.

Yukarıda anlatılanların ışığında benzetim modülünün çalışma adımları Algoritma 3 ile gösterilmiştir. Geliştirilen algoritma tamamen JAVA

Algoritma 3 Benzetim Modülünün Genel Çalışma Adımları

```
kullanıcıları yarat ve ortamı oluştur
rastgele olarak kullanıcıların çevirim içi ve çevirim dışı durumlarını ayarla
while şimdiki periyot <= maksimum periyot do
  for all tüm kullanıcılar do
    if kullanıcı çevirim içi then
      for all kullanıcının devam eden tüm oturumları do
        if yükleyici sistemde yok then
          oturumu iptal et
          yükleyicinin etkileşim değerlerini olumsuz güncelle
        else
          indirilen dosya boyutunu hesapla
          if dosya tamamlandı then
            oturumu sonlandır
            etkileşimi başarılı ya da başarısız olarak değerlendir
            yükleyicinin etkileşim değerlerini güncelle
          else if oturum süresi doldu then
            indirme işlemini iptal et
            yükleyicinin etkileşim değerlerini olumsuz güncelle
          end if
        end if
      end for
      if güven değeri güncelleme periyodu then
        kullanıcının komşularının güven değerlerini güncelle
      end if
    end if
  end for
  if kimlik değiştiren saldırganlar var ve kimlik değiştirme periyodu then
    kimlik değiştiren saldırganların kimlerini değiştir
  end if
  for all tüm kullanıcılar do
    if kullanıcı çevirim içi ve dosya indirme zamanı geldi then
      rastgele bir dosya için indirme işlemi başlat
    end if
  end for
end while
```



Şekil 5: Benzetim Sınıf Diyagramı

programlama dili ile kodlanmıştır. Şekil 5'te benzetimin sınıf diyagramı gösterilmiştir. Genel olarak, bir eş sınıfı tanımlanmış, kullanıcıların paremetreleri (indirme-gönderme bantgenişlikleri, dosyaları, indirme listeleri) bu sınıfta tutulmuş ve her bir iyi kullanıcı, saldırgan davranışına göre bu sınıftan türetilmiştir. Kullanıcılar arasında etkileşim için bir sınıf yaratılmış ve her bir etkileşim sonucu sınıf yardımıyla saklanmıştır. Benzer şekilde eşler arasında komşuluklar için de bir sınıf tanımlanmış ve komşuluk ilişkileri bu sınıf yardımıyla saklanmıştır. Ayrıca benzetim parametrelerini dosyadan okumak ve sonuçları yazmak için ayrı sınıflar oluşturulmuştur. Son olarak benzetimin tüm işleyisi için bir sınıf tanımlanmış ve Algoritma 3 bu sınıf içinde gerçekleştirilmiştir.

Algoritma 3'e göre başlangıçta tüm kullanıcılar hiçbir komşuluk ilişkisi olmadan sisteme dâhil olmaktadırlar. Benzetimin başlaması ile birlikte kullanıcılar, her bir periyotta çevirim içi durumlarına göre işlem yapmaktadırlar. Çevirim içi olan bir kullanıcı sırası geldiğinde var olan oturumlarının durumlarını güncellemektedir. İndirme yapan kullanıcı, dosyanın gerçekten istediği dosya olmasına ve herhangi bir zararlı içerik içermemesine göre dosyayı gönderen kullanıcıya olumlu güven değeri vermektedir. Aksi durumda düşük güven vermekte ve bir daha bu kullanıcı ile etkileşime girmemektedir. Bir kullanıcıya dosya gönderme isteği yapıldığında teşvik modelinin adımları uygulanıp istek kabul edilmekte veya reddedilmektedir. Dosya indirme işlemi tamamlandıktan sonra eğer

kullanıcıların güven değerlerinin güncellenme periyodu ise kullanıcıların tüm komşularının güven değerleri güncellenir. Tüm kullanıcıların kendi periyotları tamamlandıktan sonra eğer sistemde kimlik değiştiren saldırgan mevcut ve kimlik değiştirme periyodu gelmiş ise bu saldırganların kimlik değiştirme işlemleri yapılır. Daha sonra, bir sonraki periyot ile ilgili çevrim içi olan tüm kullanıcılar için rastgele bir dosya seçilip indirme oturumu başlatılmaktadır. Kullanıcılar rastgele seçtikleri bir dosyayı indirecekleri zaman dosyayı indirecekleri kullanıcı olarak önceliklerini komşularına vermektedirler. Komşuları arasında güven değerine göre yapacakları bir sıralama ile en güvendikleri komşularından dosya indirme oturumu başlatmaktadırlar. Eğer indirilecek dosya komşularda bulunamaz ise yabancı kullanıcılar ile oturum başlatılmaktadır. Kullanıcı, indirilecek dosyaya sahip yabancı kullanıcılar için kendi komşularından tavsiyeler almakta ve güven değerini hesaplayarak en güvenli gördüğü yabancı kullanıcı ile oturum başlatmaktadır. Benzetim bundan sonra bir sonraki periyoda geçmekte ve işlemler tüm periyotlar sonlanana kadar aynı şekilde devam etmektedir

5.1 Kötü Niyetli Kullanıcı Türleri

Benzetimimizde daha önceden dediğimiz gibi iyi niyetli kullanıcıların yanında tüm kullanıcıların %20'si oranında kötü niyetli kullanıcılar da bulunmaktadır. Benzetimde elde edilen sonuçlara geçmeden önce kötü niyetli kullanıcı türlerinden ve bu kullanıcıların davranışlarından bahsetmek gerekmektedir.

Sistemde iyi niyetli kullanıcılar kendisine gelen indirme isteklerini teşvik modelinin izin verdiği ölçüde kabul eden ve sistemden fayda sağlamasının yanında sisteme de fayda sağlayan kullanıcılardır. Kötü niyetli kullanıcılar ise, kendi davranışlarına göre sistemden mümkün olduğunca fayda sağlayıp; sisteme katkı vermeyen veya çok az veren kullanıcılardır. Ayrıca

kötü niyetli kullanıcılar teşvik modelini kandırmaya çalışarak da sistemden daha fazla yararlanma yoluna gidebilirler.

Sistemde 3 temel başlık altında 12 çeşit bedavacı olarak nitelendirdiğimiz kötü niyetli kullanıcı türü bulunmaktadır. Sistem bulunan bu kötü niyetli kullanıcı türleri ve geliştirilen modeller doğrultusunda bu saldırı sonuçlarındaki beklentiler sonraki alt bölümlerde anlatılmıştır.

5.1.1 Bireysel Saldırganlar

Bireysel saldırganlar, sistemde bulunan teşvik modelini kendi başına hareket ederek alt etmeyi hedefleyen ana saldırgan türüdür. Bu saldırganlar sisteme dahil olduktan sonra sahip olduğu davranışa göre hareket eder ve başka saldırganlar ile herhangi bir birliktelik oluşturmazlar.

Geliştirilen modeller çerçevesinde daha ilk aşama olan paylaşım oranı modeli ile dahi bu kötü niyetli kullanıcıların engellenebilmesi beklenmektedir. Doğal olarak güven tabanlı ve güven tabanlı uyarlanabilir modellerle de bu kötü niyetli kullanıcıların engellenebilmesi beklenmektedir. Paylaşım oranı modeli ile birlikte bu kötü niyetli kullanıcıların sadece sisteme sağladığı katkı oranında sistemden fayda sağlayabilmesi beklenmektedir. Aynı şekilde, güven tabanlı ve güven tabanlı uyarlanabilir modellerle de bu kötü niyetli kullanıcıların sadece sisteme sağladığı katkı oranında sistemden fayda sağlayabilmesi ve bu katkıyı büyük çoğunlukla gönderme yaptıkları eşlerden sağlayabilmesi beklenmektedir. Güven tabanlı model ile birlikte bir kullanıcıya dosya yolladıktan sonra onun ile komşu olunmaktadır. Ne kadar çok komşu elde edilirse servis alma olasılığı artmaktadır. Bu kullanıcılar belli bir oransal olasılıkla dosya paylaştıklarından komşu sayıları düşük olacağından bazı kullanıcılardan güven değeri yetersizliği sebebiyle de reddedileceklerdir. Herhangi bir içerik paylaşmadan sadece indirme yapmaya çalışan kullanıcılar ise, sistemden sadece ilk indirme hakları doğrultusunda yararlanabilecekler ve başka dosya indiremeyeceklerdir.

Bireysel saldırgan ana başlığı altında çeşitli davranışlar gösteren 4 tane saldırgan çeşidi bulunmaktadır.

- **Bireysel Saf Bedavacı Saldırgan:** Sistemde bulunan kötü niyetli kullanıcı türlerinden ilkidir. Bu saldırgan türünün temel davranışı sisteme dahil olduktan sonra sürekli olarak diğer kullanıcılardan dosya indirmeye çalışırken, hiçbir kullanıcıya herhangi bir dosya paylaşmamaktadır. Sistemdeki tek amacı sistemden olabildiğince kar elde etmek ve bunun karşılığında herhangi bir şey vermemektir. Sistemde bulunan bu kötü niyetli kullanıcı türü tamamen uç noktada bir davranış göstermektedir.

- **Bireysel Rastgele Bedavacı Saldırgan:** Saf bedavacı saldırganına göre paylaşım olasılığı bulunan bir saldırgan çeşididir. Bu saldırgan türünün temel davranışı sisteme dahil olduktan sonra sürekli olarak dosya indirmeye çalışırken, sisteme belli bir olasılık ile katkıda bulunurlar. Bu türdeki kötü niyetli kullanıcılara herhangi bir dosya paylaşım isteği geldiğinde bir zar atma olayı gerçekleştirirler ve %20 olasılık ile bu isteğe olumlu %80 olasılıkla olumsuz cevap verirler. Böyle bir davranış sonrasında bu kullanıcılar belli bir oranda içerik paylaşabilir ancak isteklerin büyük çoğunluğu reddedilmektedir.

- **Bireysel Değişken Bedavacı Saldırgan:** İsminden anlaşılacağı üzere davranışında sürekli olarak değişkenlik gösteren bir saldırgandır. Bu saldırgan türünün temel davranışı sisteme dahil olduktan sonra sürekli olarak dosya indirmeye çalışırken, sisteme katkı da bulunma yani dosya gönderme veya göndermeme durumları zaman içerisinde değişkenlik gösterir. Bu kötü niyetli kullanıcılara herhangi bir dosya paylaşım isteği geldiğinde bulunduğu duruma göre olumlu veya olumsuz cevap verirler. Bu saldırgan gelen ilk 80 isteği reddettikten sonra davranışında değişikliğe giderek daha sonraki gelen ilk 20 isteği kabul eder. 20 istek kabul ettikten sonra tekrar

reddetme periyoduna girer ve tüm süreç böyle devam eder. Böyle bir davranış sonrasında bu kullanıcılar belli bir oranda içerik paylaşabilir ancak isteklerin büyük kısmı reddedilecektir.

- **Bireysel Ayrımcı Bedavacı Saldırgan:** Sistemdeki kullanıcılar arasında dosya paylaşımı yönünden ayrımcılık yapan saldırgandır. Bu saldırgan türünün temel davranışı sisteme dahil olduktan sonra sürekli olarak dosya indirmeye çalışırken, sistemde kendilerinin belirledikleri belirli kullanıcılara veya kullanıcı grubuna dosya paylaşımı yaparlar. Bu kötü niyetli kullanıcılara herhangi bir dosya paylaşım isteği geldiğinde isteği yapan kullanıcının paylaşım yapılacak olarak seçilmiş listede olup olmaması duruma göre olumlu veya olumsuz cevap verirler. Bu saldırgan sisteme dahil olduktan sonra rastgele 100 kullanıcı seçer ve sadece kullanıcılardan gelen her dosya indirme isteğini kabul ederken diğer kullanıcıların isteklerini reddeder. Böyle bir davranış sonrasında bu kullanıcılar belli bir oranda içerik paylaşabilir ancak seçilen kullanıcıların dışındaki tüm istekler reddedilmektedir.

5.1.2 İşbirlikçi Saldırganlar

İşbirlikçi saldırganlar, sistemde bulunan teşvik modelini kendi aralarında iş birliği yaparak alt etmeyi hedeflerler. Bu saldırganlar, gerçek hayatta hafta da iki kereye denk gelecek aralıklarda kendi aralarında işbirliğine giderek birbirlerine dosya gönderip indirdiklerini gösterirler. Böylece dosya paylaşmış gibi görünmeyi hedefleyerek modeli alt etmeye çalışırlar. Bu çeşit saldırganlar aynı zamanda çoklu kimlik tanımla problemini de modellemektedir.

Sadece eşlerin içerik paylaşma ve indirme miktarlarına dayanan paylaşım oranı modelinin, bu saldırgan türü ile birlikte alt edilmesi beklenmektedir. Çünkü saldırganlar işbirliği sayesinde kendi paylaşım

oranlarını yükseltebilecek ve eşik orandan büyük bir paylaşım oranına sahip olabileceklerinden model bu saldırganların gerçekten paylaşım yaptığını düşünerek saldırganlara indirme için izin verecektir. Ancak güven tabanlı ve güven tabanlı uyarlanabilir modellerle birlikte bu kötü niyetli saldırganların engellenebilmesi beklenmektedir. Güven tabanlı ve uyarlanabilir tabanlı modellerle, güven metriklerinin kullanılması ile birlikte indirme yapacak kullanıcıların kendilerinin güvenilir olduğunu kanıtlaması gerekmektedir. Saldırganlar güven tabanlı modeller ile birlikte paylaşımda bulundukça diğer eşlerle komşuluk kurmaktadır. Paylaşımda bulunmayan bir eş herhangi bir komşuluk kuramamaktadır. Güven tabanlı modellerle bir dosya indirilmek istendiğinde teşvik modeli kurulan komşuluklara göre güven değeri hesaplanmakta ve buna göre dosya indirmeye izin vermekte veya reddetmektedir. Saldırganlar işbirliği içinde bulunup kendi aralarında paylaşımda bulunduklarını gösterseler dahi, gerçekten iyi niyetli kullanıcılara paylaşımda bulunmadan herhangi komşuluk kuramayacaklardır. Bu sebeple de saldırganlar iyi niyetli kullanıcılardan dosya indirmek istediklerinde güven tabanlı modeller tarafından reddedilecektirler. Modellerin tasarımı doğrultusunda her kullanıcıya ilk dosya indirme hakkı ücretsiz yani herhangi bir teşvik modeli kısıtlaması olmadan sağlanmaktadır. Sistemde hiçbir dosya paylaşımında bulunmayan saldırganın sadece bu indirme hakkından dolayı tek bir dosya indirmesi ve herhangi bir içerik paylaşmamasından dolayı modeller tarafından başka indirme yapmasına izin verilmemesi beklenmektedir. Modellerin en kötü durumda sistemdeki en büyük boyuttaki dosyayı indirebilecek bu kötü niyetli kullanıcıyı engellemesi beklenmektedir.

İşbirlikçi saldırgan ana başlığı altında, bireysel saldırganlarda olduğu gibi 4 tane saldırgan çeşidi bulunmaktadır. Bunlar işbirlikçi saf bedavacı saldırgan, işbirlikçi rastgele bedavacı saldırgan, işbirlikçi değişken saldırgan ve işbirlikçi ayrımcı bedavacı saldırgandır. Bu saldırgan çeşitleri, temelde bireysel saldırgan çeşitleri ile aynı davranışları gösterirken, işbirliği yapmalarından dolayı farklılaşmışlardır. Örneğin, işbirlikçi rastgele bedavacı saldırganı, aynı bireysel rastgele saldırganı gibi %20 olasılık ile dosya

indirme isteklerine olumlu %80 olasılıkla olumsuz cevap verirken ekstradan kendi içinde işbirliğinde de bulunmaktadır.

5.1.3 Kimlik Değiştiren Saldırgan

Kimlik değiştiren saldırgan, sistemdeki saldırganların en sonuncusudur. Diğer saldırganlardan farklı olarak sistemde saldırılarını isminden de anlaşılacağı gibi bedavacılık üzerine değil kimlik değiştirme ile yapmaktadır. Sistemde belirlenen sürelerde bir kimliğini değiştirerek, eski geçmişinden ve dolayısı ile teşvik modelinin uyguladığı cezalardan kurtulmaya çalışır. Benzetimde kimlik değiştirme süresi gerçek hayata uyarlandığında haftalık olacak şekilde ayarlanmıştır. Birçok eşler arası ağ paylaşım siteleri üyelik ile çalışmakta ve üyeliklerini belirli dönemlerde belirli süre içerisinde kabul etmektedir. Böylece kimlik değiştirme saldırılarının önüne geçmeye çalışmaktadır. Böyle kurgulanmış bir sistem için belirlediğimiz kimlik değiştirme süresi çok fazla olsa dahi amacımız mümkün olduğunca kimlik değiştiren bir saldırgan yaratarak sistemi test etmektir.

Sistemde bulunan kimlik değiştiren saldırgan, mümkün olduğunca çok sistemden dosya indirmeye çalışırken sisteme de herhangi bir katkı da bulunmamaktadır. Benzetim esnasında belirli sürelerde bir saldırgan kimliğini değiştirerek sisteme yeni bir kullanıcı gibi tekrar katılmaktadır. Böyle bir davranışta eski geçmiş verileri sıfırlanmakta ve sistemden tekrardan bir dosya indirme hakkına sahip olmaktadır. Geliştirilen modeller çerçevesinde ilk aşama olan paylaşım oranı modeli ile bu kötü niyetli kullanıcının başarılı bir şekilde engellenebilmesi beklenmemektedir. Sadece indirme ve gönderme metriklerine dayalı olan bu model ile kullanıcı her kimlik değiştirdiğinde bu metrikleri sıfırlanacak ve kullanıcı tamamen geçmişini kaybedecektir. Ancak güven tabanlı modellerle bu kötü niyetli kullanıcının engellenebilmesi beklenmektedir. Güven tabanlı model ile birlikte sisteme her katılmada kullanıcı sistemdeki tüm kullanıcılara yabancı

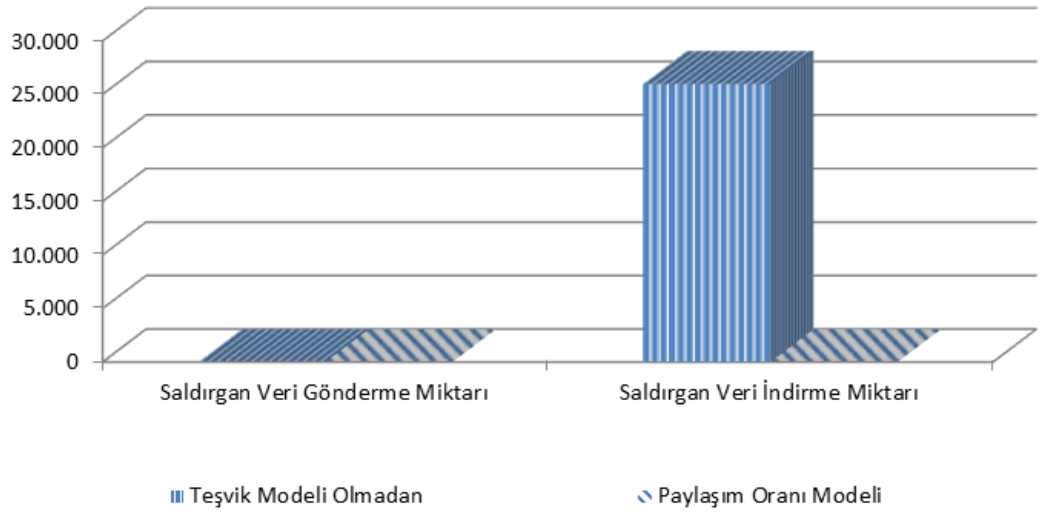
konumundadır. Sistem içerisinde ilk dosyasını indirdikten sonra ve elindeki dosyaları paylaştıkça komşuluk ilişkileri geliştirmektedir. Kimlik değiştirme sonrasında kullanıcı mevcut komşuluk ilişkilerini kaybedecek ve tekrardan yabancı konumuna düşecektir. Bu nedenle saldırgan tekrardan sisteme kendisini tanıtmalı ve kanıtlamak zorundadır. Bu sebeplerden dolayı bu saldırganın güven tabanlı modellerle engellenmesi ve kimlik değiştirmemeye karşı da bir teşvik olması beklenmektedir.

5.2 Paylaşım Oranı Modeli İle Deneyler

Paylaşım oranı modeli, kimlik değiştiren saldırgan hariç tüm saldırganlar benzetim yardımı ile test edilmiştir. Model bireysel saldırganlarda başarılı kabul edilebilir olmasına rağmen işbirlikçi saldırganlar tarafından alt edilmiştir. Bu durum beklenen bir durum olduğundan ve asıl amacımızın güven tabanlı bir model geliştirmek olduğundan bir sorun yaratmamaktadır. Paylaşım oranı modeli bize güven tabanlı bir model için sadece bir temel oluşturmuştur.

5.2.1 Bireysel Saf Bedavacı Saldırgan İle Deneyler

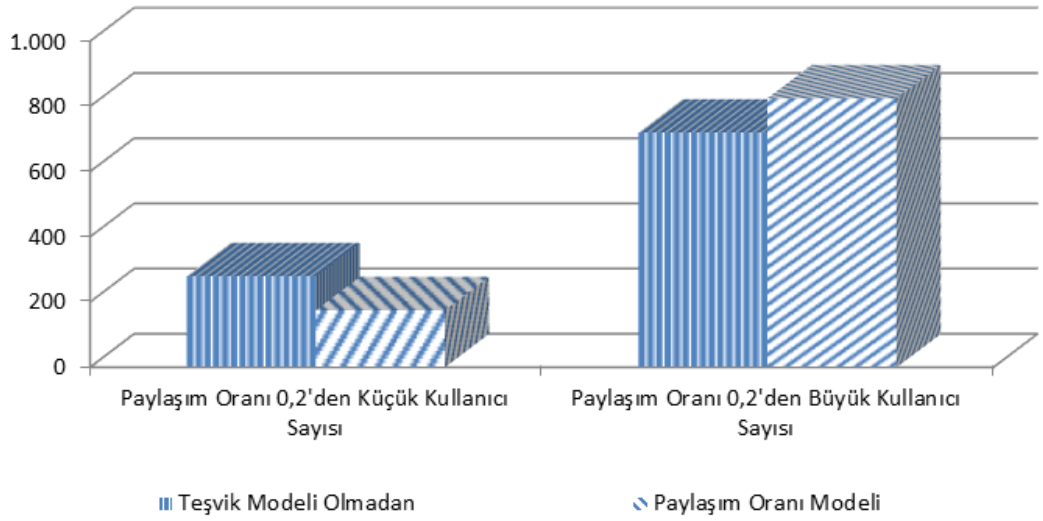
Şekil 6 paylaşım oranı modeli ile benzetimi yapılmış bireysel bedavacı saldırganının veri indirme ve gönderme miktarlarının teşvik modelsiz ve paylaşım oranı modeli ile sonuçlarını göstermektedir. Sonuçlar ortalama bir saldırganın benzetim süresince, indirdiği ve gönderdiği veri miktarını megabyte olarak göstermektedir. Şekil 6 üzerinde görülebileceği gibi, saldırgan tamamen kendi davranışını gerçekleştirerek teşvik modelinin olmadığı bir ortamda sadece veri indirmeye çalışmış ve herhangi bir veri göndermemiştir. Yani sistemden olabildiğince faydalanırken sisteme herhangi bir katkı sağlamamıştır. Ancak paylaşım oranı modeli ile birlikte saldırgan tamamen engellenmiştir. Saldırgan model ile birlikte davranışı



Şekil 6: Bireysel Saf Bedavacı Saldırganı Veri İndirme ve Gönderme Miktarları (MB)

gereği yine bir veri göndermemesinden dolayı sistemden sadece tek bir dosya indirme hakkını kullanabilmiştir. Saldırgan tamamen model tarafından engellenmiştir. Teşvik modelinin olmadığı ortamda bir saldırgan benzetim boyunca ortalama 1000 dosya indirip 0 dosya gönderirken, paylaşım oranı modeli ile saldırgan sadece 1 dosya indirebilmiş ve davranışı gereği herhangi bir dosya paylaşmamıştır.

Şekil 7 bireysel saf bedavacı saldırgan için benzetim sonunda teşvik modelsiz ve paylaşım oranı modeli tüm eşlerin paylaşım oranlarının karşılaştırmasını göstermektedir. Benzetim sonunda tüm eşlerin toplam veri gönderme miktarı ile toplam veri indirme miktarı oranlanmış ve her bir eşin paylaşım oranı bulunmuştur. Daha sonra paylaşım oranları, sistemdeki eşik oran ile karşılaştırılmıştır. Buna göre, teşvik modeli olmadığında tüm saldırganlara ek olarak bazı iyi niyetli kullanıcılar dahi eşik oran değerinin altında kalmışlardır. Bu durum normal ve beklenen bir durumdur. Teşvik modelinin olmadığı bir ortamda iyi niyetli kullanıcılar dosya paylaşmaya eğilimli olsalar dahi veri gönderme için seçilmedikleri sürece veri gönderme metriklerini artıramayacaklar ve dosya indirmek için önlerinde de bir engel olmadığı için eşik oran değerinin altında kalacaklardır. Ancak paylaşım oranı modeli ile birlikte görüldüğü üzere sadece saldırganlar

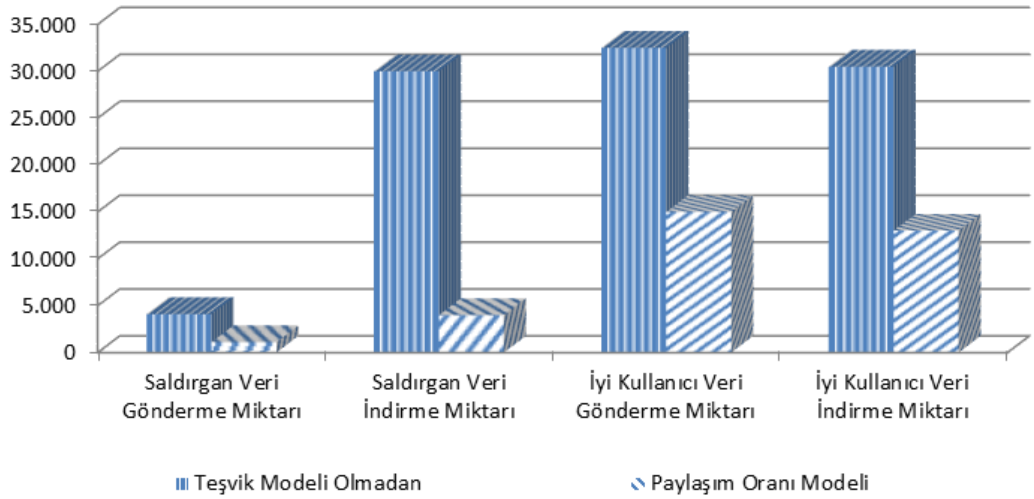


Şekil 7: Bireysel Saf Bedavacı Saldırganı Benzetimi Tüm Kullanıcıların Paylaşım Oranı Karşılaştırması

eşik oran değerinin altında kalmışlardır. Bu durum saldırganların herhangi bir dosya paylaşmamasından ve ilk indirme haklarını kullanmasından kaynaklanmaktadır. Tüm iyi niyetli kullanıcılar eşik oran değerinin üzerinde paylaşım oran değerine sahip olmuşlardır.

5.2.2 Bireysel Rastgele Bedavacı Saldırgan İle Deneyler

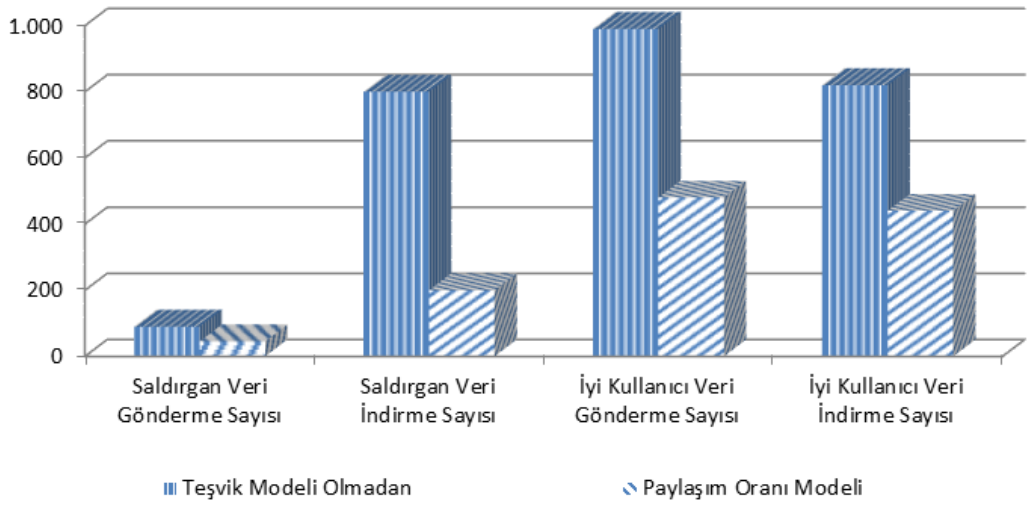
Şekil 8 bireysel rastgele saldırganının veri indirme ve gönderme miktarlarının teşvik modelsiz ve paylaşım oranı modeli ile sonuçlarını göstermektedir. Sonuçlar ortalama bir saldırganın ve iyi niyetli kullanıcının indirdiği ve gönderdiği veri miktarını megabyte olarak göstermektedir. Şekil 8 üzerinde görülebileceği gibi, saldırgan herhangi bir teşvik modelinin olmadığı durumda sistemden mümkün olabildiğince çok yararlanmış ancak sisteme davranışı gereği çok az oranda fayda sağlamıştır. Paylaşım oranı modeli ile birlikte kötü niyetli kullanıcıların sistemi sömürmesi engellenmiştir. Kötü niyetli kullanıcı sisteme sağladığı fayda ölçüsünde sistemden yararlanmıştır. Şekil 8 üzerinde yine görüldüğü üzere normal kullanıcıların veri gönderme ve indirme miktarlarında da düşmeler bulunmaktadır. Aslında bu durum bir teşvik modeli için normal bir durumdur. Bir teşvik



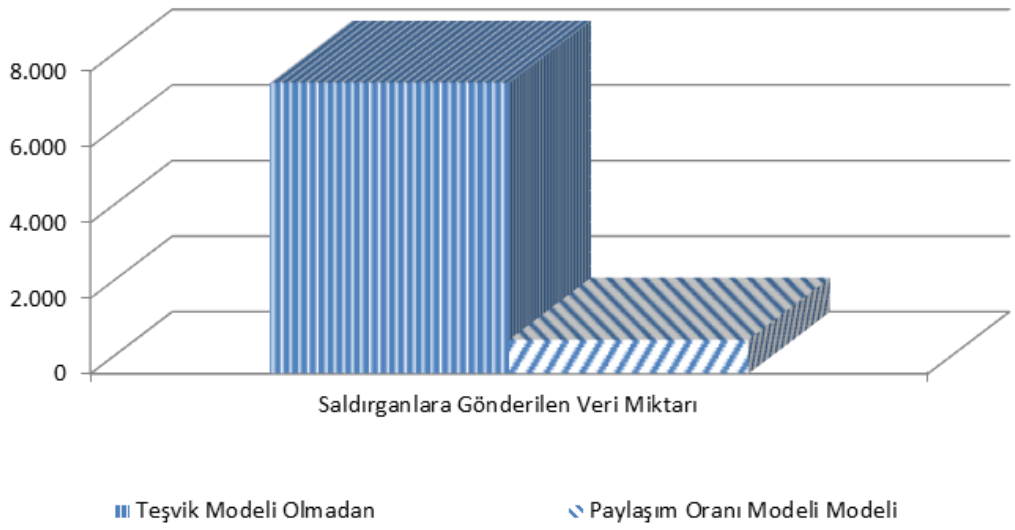
Şekil 8: Bireysel Rastgele Bedavacı Saldırganı Veri İndirme ve Gönderme Miktarları (MB)

modelinin varlığı ile sadece kötü niyetli kullanıcılar değil tüm kullanıcılar bir denetim mekanizmasının parçası olmuşlardır. Bu nedenle tüm kullanıcılar bulundukları duruma bağlı olarak veri indirebilmektedirler. Ayrıca kötü niyetli kullanıcıların engellenmesi ile birlikte kötü niyetli kullanıcıların indirdiği verileri gönderen iyi niyetli kullanıcılar belli bir veri gönderme miktarı kaybetmişlerdir. Bu durum aşağıda daha detaylı olarak anlatılmıştır.

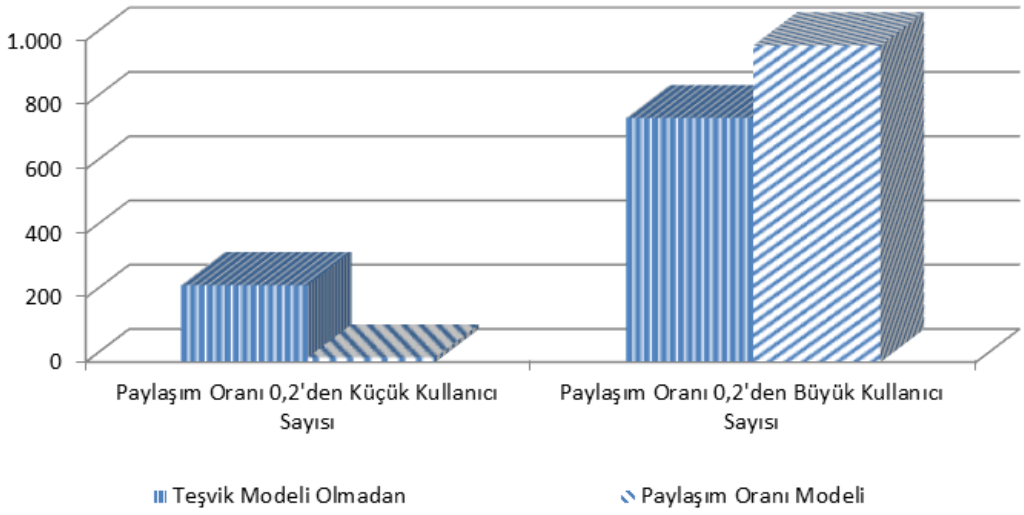
Şekil 9 bireysel bedavacı saldırganının ve iyi niyetli bir kullanıcının dosya indirme ve gönderme sayılarını teşvik modelsiz ve paylaşım oranı modeli ile sonuçlarını göstermektedir. Şekil 9 sonuçlara başka bir bakış açısı da getirmektedir. Teşvik modelinin olmadığı ortamda bir saldırgan benzetim boyunca ortalama 800 dosya indirip 90 dosya gönderirken, paylaşım oranı modeli ile saldırgan ortalama 200 dosya indirebilmiş ve 40 dosya paylaşmıştır. İyi niyetli kullanıcılar da teşvik modelinin gelmesi ile dosya indirme ve gönderme sayılarında düşme yaşamışlardır. Bir denetim sisteminin gelmesi ve kötü niyetli kullanıcıların engellenmesi sebebiyle dosya gönderme sayısında düşüşün birinci sebebidir. Ancak iyi niyetli kullanıcıların dosya gönderme ve indirme sayılarının birbirlerine oranında bir değişiklik gözükmemektedir.



Şekil 9: Bireysel Rastgele Bedavacı Saldırganı Dosya İndirme ve Gönderme Sayıları



Şekil 10: Benzetim Boyunca Bireysel Rastgele Bedavacı Saldırganına Yollanan Veri Miktarı



Şekil 11: Bireysel Rastgele Bedavacı Saldırganı Benzetimi Tüm Kullanıcıların Paylaşım Oranı Karşılaştırması

Şekil 10 iyi niyetli kullanıcılar tarafından bireysel rastgele bedavacı saldırganına yollanan veri miktarlarını göstermektedir. Bu şekil saldırganın teşvik modeli olmadan ve paylaşım oranı modeli yardımıyla ne kadar yararlanabildiğini göstermektedir. Teşvik modelinin kullanılması ile saldırganın sistemden yararlanması %80 oranında azalmıştır. Bu durum modelin saldırganı açıkça engelleyebildiğini göstermektedir. Ayrıca saldırgan teşvik modelinin olmadığı durumda indirebildiği verileri, teşvik modeli ile indirememektedir. Tüm bu durum iyi niyetli kullanıcıların da veri gönderme miktarlarında azalmaya aynı şekilde doğru orantılı olarak da iyi niyetli kullanıcıların veri indirme miktarlarında da azalmaya yol açmaktadır. İyi niyetli kullanıcıların veri gönderme miktarlarındaki düşüşün ikinci büyük bir sebebi bu durumdur.

Şekil 11 benzetim sonunda teşvik modelsiz ve paylaşım oranı modeli tüm kullanıcıların paylaşım oranlarının karşılaştırmasını göstermektedir. Buna göre, teşvik modeli olmadığında tüm saldırganlara ek olarak bazı iyi niyetli kullanıcılar dahi eşik oran değerinin altında kalmışlardır. Bu durum normal ve beklenen bir durumdur. Teşvik modelinin olmadığı bir ortamda iyi niyetli kullanıcılar dosya paylaşmaya eğilimli olsalar dahi veri gönderme için seçilmedikleri sürece veri gönderme metriklerini artıramayacaklar ve

dosya indirmek için önlerinde de bir engel olmadıkları için de eşik oran değerinin altında kalacaklardır. Ancak paylaşım oranı modeli ile birlikte görüldüğü üzere sadece çok az sayıda saldırgan eşik oran değerinin altında kalmıştır. Saldırganlar teşvik model tarafından paylaşıma zorlandıkları için paylaşım yapmak zorunda kalmışlardı ve büyük çoğunluğu eşik orandan büyük paylaşım oranına ulaşmışlardır. Tüm iyi niyetli kullanıcılar eşik oran değerinin üzerinde paylaşım oran değerine sahip olmuşlardır.

5.2.3 Bireysel Değişken Bedavacı Ve Bireysel Ayrımcı Bedavacı Saldırganları İle Deneyler

Çizelge 3 paylaşım oranı modeli ile benzetimi yapılmış bireysel değişken, bireysel ayrımcı saldırganlarının ve iyi kullanıcıların veri indirme, gönderme miktarlarının ve iyi kullanıcıların saldırganlara yolladıkları veri miktarlarının teşvik modelsiz ve paylaşım oranı modeli ile sonuçlarını göstermektedir. Önceki bölümdeki deney sonuçlarına paralel sonuçlar bu saldırganlar ile de görülmektedir. Herhangi bir teşvik modelinin olmadığı durumda saldırganlar kendi davranışları ölçüsünde sisteme katkı sağlarken, sistemden olabildiğince çok yararlanmaya çalışmışlardır. Teşvik modeli ile birlikte saldırganlar paylaşımları ölçüsünde sistemden yararlanabilmelerine izin verilmiştir. Teşvik modeli ile birlikte iyi niyetli kullanıcıların veri indirme ve gönderme miktarlarında düşmeler gözlenmiştir. Bu durum önceki bölümde açıklandığı gibi teşvik modelinin gelmesi ile iyi niyetli kullanıcılarında denetime dahil olması ve saldırganlara gönderilen verilerin düşmesi ile açıklanabilir. Saldırganlara gönderilen veriler iyi niyetli kullanıcıların paylaşım oranında düşmelere yol açmaktadır ve bu sebeple iyi niyetli kullanıcılar teşvik modelinin olmadığı ortamdaki kadar veri göndermesi yapamamaktadırlar. Saldırganlar teşvik modelinin olmadığı benzetimde ortalama 800 dosya indirip 75 dosya gönderirlerken, paylaşım oranı modeli ile birlikte ortalama 190 dosya indirip 55 dosya paylaşmışladır. Paylaşım Oranı Modeli ile birlikte, saldırganların hemen hemen hepsi sistem eşik

Çizelge 3: Bireysel Değişken Bedavacı Ve Bireysel Ayrımcı Bedavacı Saldırganları İle Veri İndirme ve Gönderme Miktarları

	Bireysel Değişken Bedavacı		**Bireysel Ayrımcı Bedavacı**	
	Teşvik Modelsiz	**Paylaşım Oranı Modeli**	**Teşvik Modelsiz**	**Paylaşım Oranı Modeli**
Saldırgan Veri Gönderme Miktarı(MB)	4898	3105	2849	1023
Saldırgan Veri İndirme Miktarı(MB)	28812	5232	29081	2156
İyi Kullanıcı Veri Gönderme Miktarı(MB)	31978	13423	35004	12310
İyi Kullanıcı Veri İndirme Miktarı(MB)	28746	12131	29211	12179
Saldırgana Gönderilen Veri Miktarı(MB)	7098	1105	6201	487

oranın üzerinde paylaşım oranına sahiptirler. Paylaşım için hiçbir zaman seçilmeyen ortalama 12 tane eş paylaşım yapamadıklarından paylaşım oranını artıramamışlar ve eşik oranın altında kalmışlardır. Bu eşler sadece ilk dosya indirme haklarını kullanabilmişlerdir.

5.2.4 İşbirlikçi Saldırganlar İle Deneyler

Çizelge 4 paylaşım oranı modeli ile işbirlikçi saldırganların benzetim sonuçlarını göstermektedir. Beklenildiği gibi tüm işbirlikçi saldırganlar teşvik modelini alt etmeyi başarmışlardır. İşbirlikçi saldırganlar belirli

Çizelge 4: İşbirlikçi Saldırganlar İle Veri İndirme ve Gönderme Miktarları

	Saldırgan Veri Gönderme Miktarı(MB)		**Saldırgan Veri İndirme Miktarı(MB)**	
	Teşvik Modelsiz	**Paylaşım Oranı Modeli**	**Teşvik Modelsiz**	**Paylaşım Oranı Modeli**
İşbirlikçi Saf Bedavacı Saldırgan	0	0	30099	28384
İşbirlikçi Rastgele Bedavacı Saldırgan	3544	2214	27962	26480
İşbirlikçi Değişken Bedavacı Saldırgan	3735	2453	28613	26963
İşbirlikçi Ayrımcı Bedavacı Saldırgan	4112	2516	28651	27833

aralıklarla birbirlerine dosya gönderdiklerini iddia etmektedirler. Bu sayede saldırganlar paylaşım oranlarını yükseltmişler ve gerçekte sisteme çok az katkı yaparak sistemden olabildiğince yararlanmışlardır.

5.2.5 Paylaşım Oranı Modeli İle Deney Sonuçları

Paylaşım Oranı Modeli ile bireysel ve işbirlikçi saldırganların tüm çeşitlerinin benzetimi yapılmıştır. Benzetim sonuçlarında da görüleceği üzere, paylaşım oranı modeli bireysel saldırganların hepsinde başarılı sayılabilir. Ancak işbirlikçi saldırganlar modeli kandırmayı başarmışlardır. Geliştirilen model ile birlikte iyi niyetli kullanıcılarında veri indirme ve gönderme miktarında düşmeler olmuştur. Bu düşmelerin kabul edilebilir ve beklenen oldukları düşünülmektedir. Paylaşım modelinin tek başına bir eşler arası ağ

uygulamasında kullanılması yetersiz gelecektir. Bu model bizim için temel hedefimiz olan güven tabanlı model için altyapı sağlayacaktır.

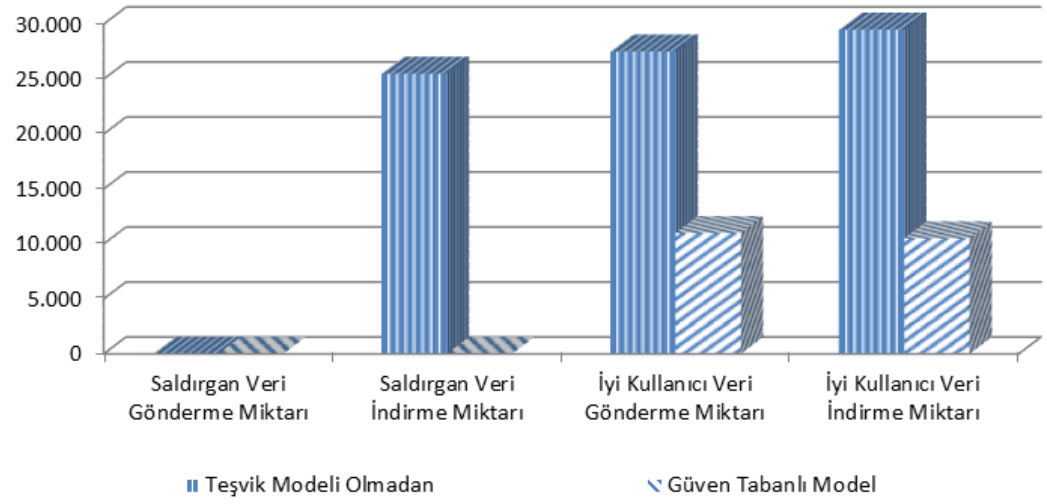
5.3 Güven Tabanlı Model İle Deneyler

Güven tabanlı model, paylaşım oranı modeli üzerine geliştirilmiş ve temelinde güven metriklerini kullanan modeldir. Daha önce bahsedildiği gibi kullanıcıların paylaştıkları içeriklerin doğru ve istenilen içerik olmasına göre güven puanları verilmektedir. Paylaşım oranının yanında bu puanları da temel bir teşvik sistemi kullanıcıların indirme yapıp yapamayacağına karar vermektedir. Güven Tabanlı Modeli ile kimlik değiştiren saldırgan hariç bireysel ve işbirlikçi tüm saldırganların benzetimi yapılmıştır. Geliştirilen model ile birlikte bireysel kullanıcıların yanında işbirlikçi saldırganlar da engellenebilmiştir. Ayrıca bireysel saf bedavacı saldırgan birebir aynı sonuçları verdiğinden bu bölümde detaylı sonuçları paylaşılmamıştır.

5.3.1 Bireysel Saldırganlar İle Deneyler

Çizelge 5: Bireysel Saldırganlar İle Veri İndirme ve Gönderme Miktarları

	Saldırgan Veri Gönderme Miktarı(MB)		**Saldırgan Veri İndirme Miktarı(MB)**	
	Teşvik Modelsiz	**Güven Tabanlı Model**	**Teşvik Modelsiz**	**Güven Tabanlı Model**
Saf Bedavacı	0	0	26221	0
Rastgele Bedavacı	3904	1055	30000	3413
Değişken Bedavacı	4925	1234	28112	4242
Ayrımcı Bedavacı	2109	426	28261	1711



Şekil 12: İşbirlikçi Saf Bedavacı Saldırganı Veri İndirme ve Gönderme Miktarları (MB)

Çizelge 5 güven tabanlı model ile benzetimi yapılmış bireysel saldırganların sonuçlarını göstermektedir. Bireysel saldırganların güven tabanlı model ile birlikte de engellendiği görülmektedir.

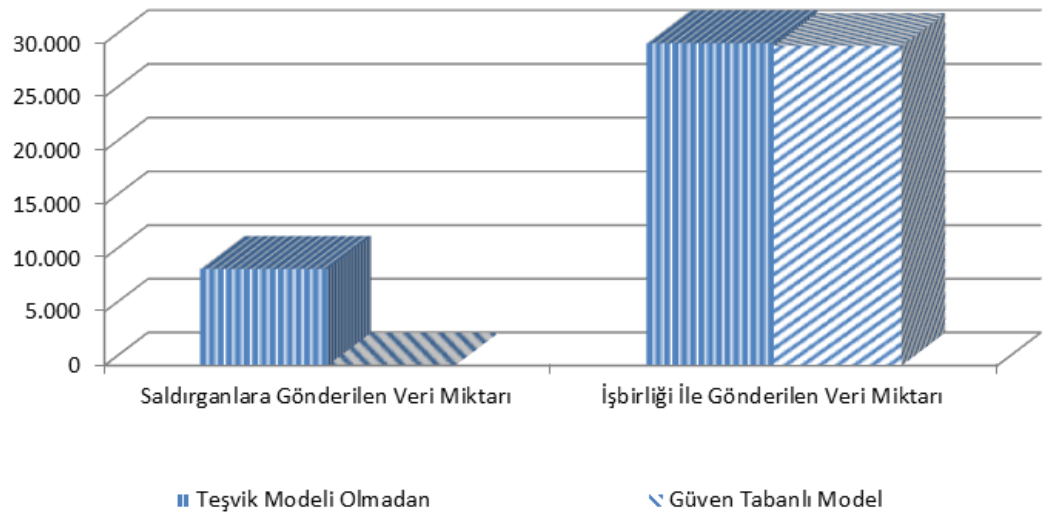
Güven tabanlı model ile birlikte, eşlerin güven metriklerinden yararlanılarak Bölüm 4.2.2'de anlatıldığı gibi bir teşvik sistemi sağlamaktadır. Güven tabanlı model, paylaşım oranı modeline göre daha fazla kontrol yapmakta ve eşleri paylaşım için daha çok zorlamaktadır. Bireysel saldırganların indirebildikleri veri miktarları, paylaşım oranı modeline göre daha da düşmektedir. Güven tabanlı model ile birlikte, saldırganlar ortalama 100 dosya indirebillirken, 23 dosya göndermişlerdir. Güven Tabanlı Model'in gücü işbirlikçi saldırganların benzetimleri ile daha da ortaya çıkmaktadır. Paylaşım oranı modeli işbirlikçi saldırganlarda başarısız olurken Güven Tabanlı Model işbirlikçi saldırganları da engellemesi beklenmektedir.

5.3.2 İşbirlikçi Saf Bedavacı Saldırgan İle Deneyler

Şekil 12 Güven Tabanlı Model ile benzetimi yapılmış işbirlikçi saf saldırganının veri indirme ve gönderme miktarlarının teşvik modelsiz ve

Güven Modeli ile sonuçlarını göstermektedir. Sonuçlar ortalama bir saldırganın ve iyi niyetli kullanıcının indirdiği ve gönderdiği veri miktarını megabyte olarak göstermektedir. Şekil 12 üzerinde görülebileceği gibi, saldırgan herhangi bir teşvik modelinin olmadığı durumda sistemden mümkün olabildiğince çok yararlanmış ancak sisteme davranışı gereği herhangi bir fayda sağlamamıştır. Güven Modeli ile birlikte kötü niyetli kullanıcıların sistemi sömürmesi engellenmiştir. Kötü niyetli kullanıcı sisteme herhangi bir fayda sağlamadığından sistemden yararlanamamıştır. Şekil 12 üzerinde yine görüldüğü üzere normal kullanıcıların veri gönderme ve indirme miktarlarında da düşmeler bulunmaktadır. Bu durum bir teşvik modeli ile aslında normal bir durumdur. Daha önce açıkladığımız gibi bir teşvik modelinin varlığı ile sadece kötü niyetli kullanıcılar değil tüm kullanıcılar bir denetim mekanizmasının parçası olmuşlardır. Ayrıca kötü niyetli kullanıcıların engellenmesi ile birlikte kötü niyetli kullanıcıların indirdiği verileri gönderen iyi niyetli kullanıcılar belli bir veri gönderme miktarı kaybetmişlerdir. Teşvik modelinin olmadığı ortamda bir saldırgan benzetim boyunca ortalama 900 dosya indirip herhangi bir dosya göndermemişken, Güven Tabanlı Model ile saldırgan herhangi bir dosya paylaşmadığından herhangi bir dosya da indirememiştir. İyi niyetli kullanıcılar da teşvik modelinin gelmesi ile dosya indirme ve gönderme sayılarında düşme yaşamışlardır. Bir denetim sisteminin gelmesi, kötü niyetli kullanıcıların engellenmesi sebebiyle dosya gönderme sayısında düşüş bu durumu açıklamaktadır. Ancak iyi niyetli kullanıcıların dosya gönderme ve indirme sayılarının birbirlerine oranında bir değişiklik gözükmemektedir.

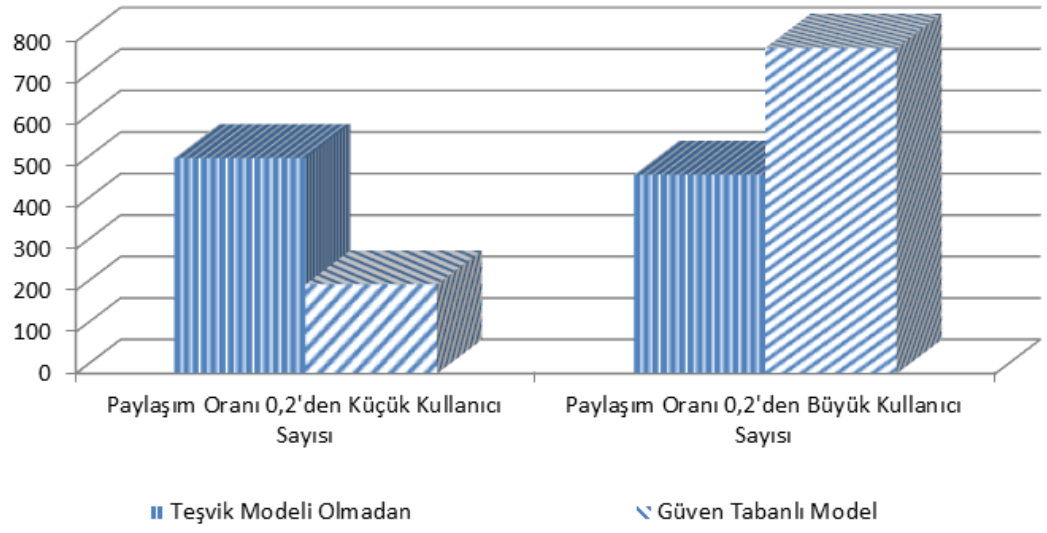
Şekil 13 iyi niyetli kullanıcılar tarafından işbirlikçi saf bedavacı saldırganına yollanan ve bir işbirlikçi saldırganın işbirliği adı altında gönderdiği veri miktarlarını göstermektedir. Bu şekil saldırganın teşvik modeli olmadan ve Güven Tabanlı Model yardımıyla ne kadar yararlanabildiğini göstermektedir. Teşvik modelinin kullanılması ile saldırganın sistemden yararlanması %100 oranında azalmıştır. Bu durum modelin saldırganı açıkça engelleyebildiğini göstermektedir. Saldırgan davranışı gereği iyi niyetli kullanıcılara herhangi



Şekil 13: Benzetim Boyunca İşbirlikçi Saf Bedavacı Saldırganına Yollanan ve İşbirliği ile Gönderilmiş Gösterilen Veri Miktarı

bir paylaşım yapmamasından dolayı iyi niyetli kullanıcılar ile herhangi bir komşuluk kuramamakta ve iyi niyetli kullanıcılardan herhangi bir veri indirememektedir. Saldırganlar teşvik modelinin olmadığı ortamda ortalama 30 GB veriyi başka saldırganlara gönderdiğini iddia ederek sistemi yanıltmaya ve paylaşım oranını artırmaya çalışmıştır. Güven Tabanlı Model ile birlikte benzetim boyunca paylaşım oranını artırmak için yine işbirliği paylaşımını yapmış ancak buna rağmen sistemden yararlanamadığı için ve paylaşım oranı düşmediğinden işbirlikçi paylaşımı çok az olarak gözükmüştür.

Şekil 14 işbirlikçi saf saldırganı deneyinde benzetim sonunda teşvik modelsiz ve Güven Modeli tüm kullanıcıların paylaşım oranlarının karşılaştırmasını göstermektedir. Buna göre, teşvik modeli olmadığında tüm saldırganlara ek olarak bazı iyi niyetli kullanıcılar dahi eşik oran değerinin altında kalmışlardır. Teşvik modelinin olmadığı bir ortamda iyi niyetli kullanıcılar dosya paylaşmaya eğilimli olsalar dahi veri gönderme için seçilmedikleri sürece veri gönderme metriklerini artıramayacaklar ve eşik oran değerinin altında kalacaklardır. Ancak Güven Modeli ile birlikte sadece saldırganlar eşik oran değerinin altında kalmışlardır. Bu

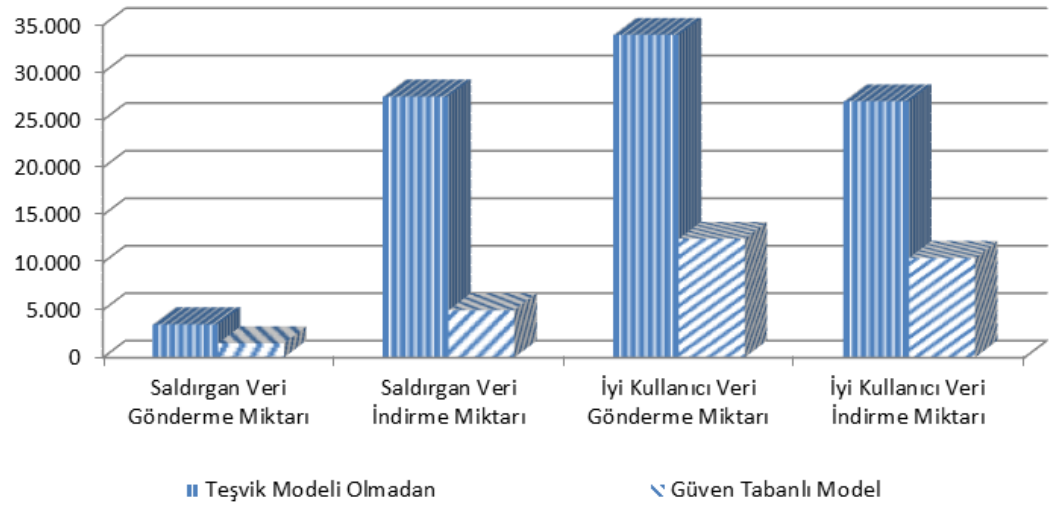


Şekil 14: İşbirlikçi Saf Bedavacı Saldırganı Benzetimi Tüm Kullanıcıların Paylaşım Oranı Karşılaştırması

durum saldırganların ilk indirme haklarını kullanıp dosya gönderme için seçilmemesinden kaynaklanmaktadır. Tüm iyi niyetli kullanıcılar eşik oran değerinin üzerinde paylaşım oran değerine sahip olmuşlardır.

5.3.3 İşbirlikçi Rastgele Bedavacı Saldırgan İle Deneyler

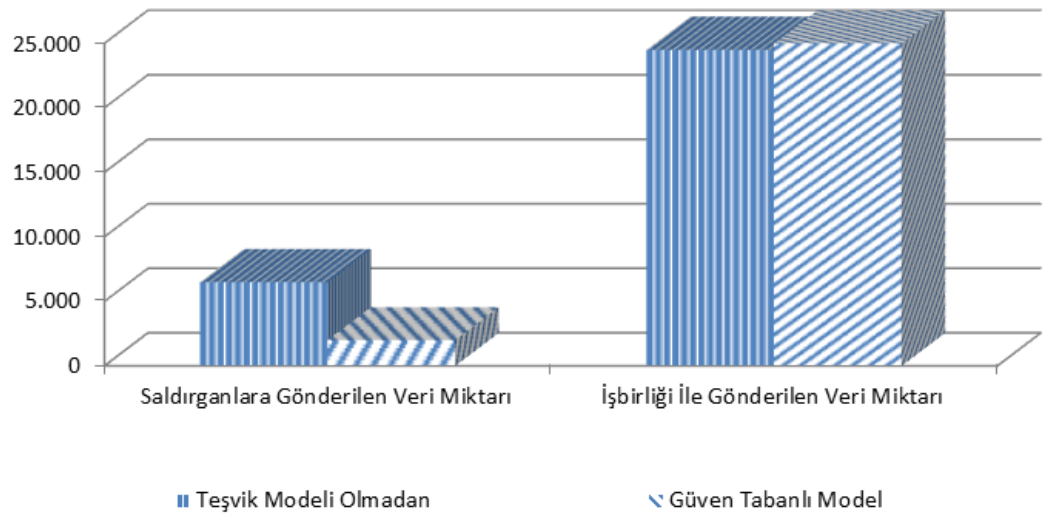
Şekil 15 Güven Tabanlı Model ile benzetimi yapılmış işbirlikçi rastgele saldırganının veri indirme ve gönderme miktarlarının teşvik modelsiz ve Güven Modeli ile sonuçlarını göstermektedir. Saldırgan herhangi bir teşvik modelinin olmadığı durumda sistemden mümkün olabildiğince çok yararlanmış ancak sisteme davranışı gereği çok az fayda sağlamıştır. Güven Modeli ile birlikte kötü niyetli kullanıcıların sistemi sömürmesi engellenmiştir. Kötü niyetli kullanıcı sisteme çok az fayda sağladığından sistemden çok az yararlanabilmiştir. Şekil 15 üzerinde yine görüldüğü üzere normal kullanıcıların veri gönderme ve indirme miktarlarında da düşmeler bulunmaktadır. Bu durum bir teşvik modeli ile aslında normal bir durumdur. Bir teşvik modelinin varlığı ile sadece kötü niyetli kullanıcılar değil tüm kullanıcılar bir denetim mekanizmasının parçası olmuşlardır. Ayrıca



Şekil 15: İşbirlikçi Rastgele Bedavacı Saldırganı Veri İndirme ve Gönderme Miktarları (MB)

kötü niyetli kullanıcıların engellenmesi ile birlikte kötü niyetli kullanıcıların indirdiği verileri gönderen iyi niyetli kullanıcılar belli bir veri gönderme miktarı kaybetmişlerdir. Teşvik modelinin olmadığı ortamda bir saldırgan benzetim boyunca ortalama 900 dosya indirip herhangi 100 dosya paylaşmış iken, Güven Tabanlı Model ile saldırgan ortalama 200 dosya indirebilmiş ve 30 dosya yollamıştır. İyi niyetli kullanıcılar da teşvik modelinin gelmesi ile dosya indirme ve gönderme sayılarında düşme yaşamışlardır. Ancak iyi niyetli kullanıcıların dosya gönderme ve indirme sayılarının birbirlerine oranında bir değişiklik gözükmemektedir.

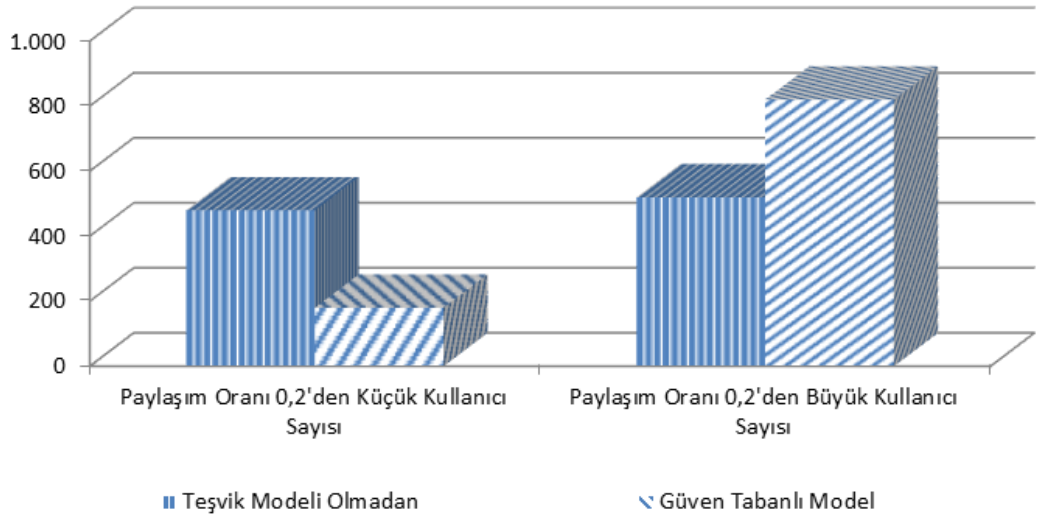
Şekil 16 iyi niyetli kullanıcılar tarafından işbirlikçi rastgele bedavacı saldırganına yollanan ve bir işbirlikçi saldırganın işbirliği adı altında gönderdiği veri miktarlarını göstermektedir. Bu şekil saldırganın teşvik modeli olmadan ve Güven Tabanlı Model yardımıyla ne kadar yararlanabildiğini göstermektedir. Teşvik modelinin kullanılması ile saldırganın sistemden yararlanması %70 oranında azalmıştır. Bu durum modelin saldırganı açıkça engelleyebildiğini göstermektedir. Saldırganlar teşvik modelinin olmadığı ortamda ortalama 24 GB veriyi başka saldırgana gönderdiğini iddia ederek sistemi yanıltmaya ve paylaşım oranını artırmaya çalışmıştır. Güven Tabanlı Model ile birlikte benzetim boyunca paylaşım



Şekil 16: Benzetim Boyunca İşbirlikçi Rastgele Bedavacı Saldırganına Yollanan ve İşbirliği ile Gönderilmiş Gösterilen Veri Miktarı

oranını artırmak için yine ortalama 25 GB veriyi başkalarına gönderdiğini iddia etmiş ancak buna rağmen sistemi kandırmamış ve sistemden fayda sağlayamamıştır.

Şekil 17 işbirlikçi rastgele saldırganı deneyinde benzetim sonunda teşvik modelsiz ve Güven Modeli tüm kullanıcıların paylaşım oranlarının karşılaştırmasını göstermektedir. Buna göre, teşvik modeli olmadığında tüm saldırganlara ek olarak bazı iyi niyetli kullanıcılar dahi eşik oran değerinin altında kalmışlardır. Bu durum normal ve beklenen bir durumdur. Teşvik modelinin olmadığı bir ortamda iyi niyetli kullanıcılar dosya paylaşmaya eğilimli olsalar dahi veri gönderme için seçilmedikleri sürece veri gönderme metriklerini artıramayacaklar ve dosya indirmek için önlerinde de bir engel olmadıkları için de eşik oran değerinin altında kalacaklardır. Ancak Güven Modeli ile birlikte görüldüğü üzere sadece saldırganların bir bölümü eşik oran değerinin altında kalmışlardır. Bu durum da saldırganların ilk indirme haklarını kullanıp dosya gönderme için seçilmemesinden kaynaklanmaktadır. Tüm iyi niyetli kullanıcılar eşik oran değerinin üzerinde paylaşım oran değerine sahip olmuşlardır.



Şekil 17: İşbirlikçi Rastgele Bedavacı Saldırganı Benzetimi Tüm Kullanıcıların Paylaşım Oranı Karşılaştırması

5.3.4 İşbirlikçi Değişken Bedavacı ve İşbirlikçi Ayrımcı Saldırganlar İle Deneyler

Çizelge 6 güven tabanlı model ile benzetimi yapılmış işbirlikçi değişken ve ayrımcı saldırganlarının ve iyi kullanıcıların veri indirme, gönderme miktarlarının ve iyi kullanıcıların saldırganlara yolladıkları veri miktarlarının teşvik modelsiz ve paylaşım oranı modeli ile sonuçlarını göstermektedir. Önceki bölümde bulunan sonuçlara benzer sonuçlar bu iki saldırgan içinde bulunmuştur. Güven Modeli ile birlikte saldırganların sistemi sömürmesi engellenmiştir ve saldırganlar sisteme çok az fayda sağladığından sistemden çok az yararlanabilmiştir. Saldırganlar teşvik modelini yanıltabilmek için kendi aralarında yüksek miktarda veri gönderimi göstermiş olmalarına rağmen, güven tabanlı model alt edilememiştir. Herhangi bir teşvik modelinin varlığı olmaması durumuna göre güven tabanlı teşvik modeli ile birlikte iyi niyetli kullanıcılar da veri gönderme ve indirme miktarlarında düşmeler yaşamışlardır. Teşvik modeli ile birlikte iyi niyetli kullanıcılar da kendilerini birbirlerine kanıtlamak zorundadırlar. Bu kanıtlama sürecinde, teşvik modelinin olmaması durumuna göre daha az sistemden yararlanabilmektedirler. Ancak bu süreç ilerledikçe

Çizelge 6: İşbirlikçi Değişken Bedavacı ve İşbirlikçi Ayrımcı Saldırganlar İle Veri İndirme ve Gönderme Miktarları

	İşbirlikçi Değişken Bedavacı		**İşbirlikçi Ayrımcı Bedavacı**	
	Teşvik Modelsiz	**Güven Tabanlı Model**	**Teşvik Modelsiz**	**Güven Tabanlı Model**
Saldırgan Veri Gönderme Miktarı(MB)	3759	1628	3997	1355
Saldırgan Veri İndirme Miktarı(MB)	28462	5311	27818	5761
İyi Kullanıcı Veri Gönderme Miktarı(MB)	34995	14121	35000	14851
İyi Kullanıcı Veri İndirme Miktarı(MB)	27369	12335	26847	12009
Saldırganlara Gönderilen Veri Miktarı(MB)	7003	2544	7518	2500

kullanıcı sistemden daha çok yararlanabilmektedir. Ayrıca kötü niyetli kullanıcılara yollanan verinin azalması iyi niyetli kullanıcılarında veri gönderme miktarlarını dolayısı ile veri indirme miktarlarını düşürmektedir. Teşvik modelinin olmadığı ortamda bir saldırgan benzetim boyunca ortalama 900 dosya indirip herhangi 95 dosya paylaşmış iken, Güven Tabanlı Model ile saldırgan ortalama 200 dosya indirebilmiş ve 40 dosya yollamıştır.

Saldırganlar işbirliği çerçevesinde birbirlerine veri gönderdiklerini iddia ederek teşvik modelini kandırmayı amaçlamışlardır. Saldırganlar teşvik modelinin olmadığı ortamda ortalama 25 GB veriyi başka saldırgana

gönderdiğini iddia ederek sistemi yanıltmaya ve paylaşım oranını artırmaya çalışmışlardır. Güven Tabanlı Model ile birlikte benzetim boyunca paylaşım oranını artırmak için yine ortalama 22 GB veriyi başkalarına gönderdiğini iddia etmişler ancak buna rağmen sistemi kandırmamış ve sistemden fayda sağlayamamıştır.

5.3.5 Kimlik Değiştiren Saldırgan İle Deneyler

Kimlik değiştiren saldırgan, eşler arası ağlarda karşılaşılan en zor problemlerden biridir. Saldırgan uygulanan teşvik modelinin cezalarından kurtulmak için sistemden ayrılır ve yeni bir kimlik ile sisteme tekrar dahil olur. Bu durumda kullanıcı eski cezalarından kurtulur. Bu saldırganının engellenebilmesi için sistemdeki kullanıcıların değiştirilemez tekil tanımlayıcılar ile belirlenebilmesi gerekmektedir.

Model her kimlik değiştirme işleminde kimlik değiştiren kullanıcıyı yabancı bir kullanıcı kabul etmektedir. Bu nedenle kimlik değiştirme işleminin sonucunda kullanıcı tekrardan ilk dosya indirme hakkına sahip olmakta ancak sisteme de kendini kanıtlama zorunluluğu ile karşılaşmaktadır. Benzetim üzerinde kullanıcılar sürekli olarak kimlik değiştirir ise modeli alt edebilirler. Ancak saldırganlar kimlik değiştirme işlemini gerçek hayatta her haftada iki kere kimlik değiştirecek şekilde daha mantıklı ve gerçekleşebilir sürelerde yaptıklarında, model saldırganları engellemeyi başarabilmektedir. Birçok eşler arası ağ paylaşım sitesi kullanıcılarını kayıt işlemi ile almaktadır ve bu kayıt işlemini yılın belirli zamanlarında kısa süreliğine aktif hale getirmektedir. Bu sayede kimlik değiştirme işleminin de mümkün olduğunca önüne geçilmesi hedeflenmektedir.

Güven tabanlı model ile birlikte, kimlik değiştiren saldırganın benzetimi yapılarak geçmişi silme saldırısı test edilmiştir. Bireysel rastgele, bireysel değişken, bireysel ayrımcı bedavacı saldırganlar gerçek hayatta her haftada iki kere kimlik değiştirecek şekilde benzetimi yapılmıştır.

Çizelge 7: Kimlik Değiştiren Saldırgan İle Veri İndirme ve Gönderme Miktarları

	Saldırgan Veri Gönderme Miktarı(MB)	**Saldırgan Veri İndirme Miktarı(MB)**	**İyi Kullanıcı Veri Gönderme Miktarı(MB)**	**İyi Kullanıcı Veri İndirme Miktarı(MB)**
Rastgele Bedavacı - Teşvik Modelsiz	4215	29968	32651	28045
Rastgele Bedavacı - GT Model	1012	7356	10841	8944
Değişken Bedavacı - Teşvik Modelsiz	4806	28634	30999	27915
Değişken Bedavacı - GT Model	1192	8530	11205	9166
Ayrımcı Bedavacı - Teşvik Modelsiz	2917	29845	35766	30044
Ayrımcı Bedavacı - GT Model	998	6502	10736	9109

Çizelge 7 güven tabanlı model ile kimlik değiştiren saldırganların ve iyi kullanıcıların veri indirme ve gönderme miktarlarını göstermektedir. Saldırganlar kimlik değiştirme işlemine rağmen iyi kullanıcılar kadar sistemden yararlanamamışlardır. Saldırganlar kimlik değiştirerek sürekli olarak ilk dosya indirme haklarından yararlanabildiklerinden sistem eşik oranının altında paylaşım oranlarına sahiptirler. Sistem üzerinde kimlik değiştiren saldırganlar sadece kötü geçmişlerini değil aynı zamanda komşuluklarını da kaybederler. Bu nedenle ilk dosya indirme sonrası dosya indirebilme ihtimalleri de azalmaktadır. Güven modeli bu yapısı ile kimlik değiştiren saldırganlar üzerinde kısmen de olsa başarılı olduğu kabul

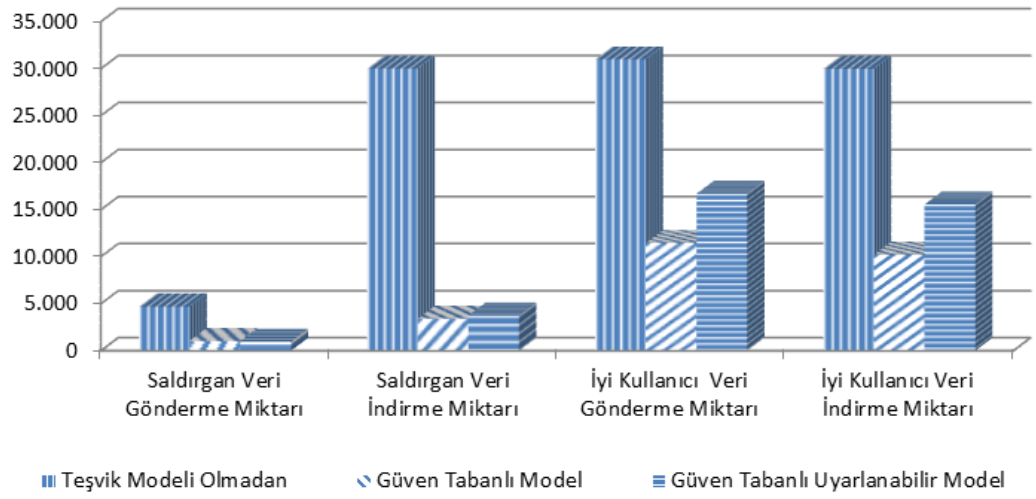
edilebilir.

5.3.6 Güven Tabanlı Model İle Deney Sonuçları

Güven tabanlı modelde, paylaşım oranı modelinin üzerine güven metriklerini kullanan bir teşvik sisteminin eklenmiştir. Paylaşım oranı modeli bireysel saldırganları engelleyebilmişken, işbirlikçi saldırganlar tarafından alt edilmiştir. Güven tabanlı model ile tüm saldırgan türlerinin benzetimi yapılmış ve model saldırganların sistemi sömürmesini engellemeyi başarmıştır. Modelin farklılığı ve başarısı işbirlikçi saldırganların benzetimlerinde daha da ortaya çıkmıştır. Paylaşım oranı modelinin aksine bu model işbirlikçi saldırganları da engellemeyi başarmıştır. Uzun süreli güven ilişkileri sayesinde paylaşım yapmayan saldırganlar kendilerine komşu edinememişler ve bu nedenle model tarafından sistem kaynaklarından yararlanmaları engellenmiştir. Modelin tek dezavantajı, iyi niyetli kullanıcıların da denetim mekanizmasından etkilenmesi gösterilebilir.

5.4 Güven Tabanlı Uyarlanabilir Model İle Deneyler

Güven tabanlı uyarlanabilir model, iyi niyetli kullanıcıların mümkün olduğunca daha az etkilenmesi için geliştirilmiş güven tabanlı modelin son aşamasıdır. Geliştirdiğimiz teşvik model de her bir kullanıcı kendisini hem paylaşım oranı yönden hem de güven değeri yönünden kanıtlamak zorundadır. Bundan dolayı tüm kullanıcılara bir kendini kanıtlama evresi yaşamaktadırlar ve bu evre boyunca sistemden maksimum şekilde yararlanamamaktadırlar. Güven Tabanlı Uyarlanabilir Model yardımıyla bu evreyi iyi niyetli kullanıcılar için daha kolay ve daha kısa hale getirmek amaçlanmıştır. Güven Tabanlı Uyarlanabilir Model ile birlikte kötü niyetli kullanıcıların engellenmesinde herhangi bir sıkıntı karşılaşılmadan iyi niyetli kullanıcıların sistemden daha fazla fayda sağlayabilmesi sağlanmıştır. Bu



Şekil 18: Bireysel Rastgele Saldırgan Veri İndirme ve Gönderme Miktarları (MB)

model kapsamında tüm saldırganların benzetimi yapılmıştır.

5.4.1 Bireysel Rastgele Bedavacı Saldırganı

Şekil 18 Güven Tabanlı Uyarlanabilir Model ile benzetimi yapılmış bireysel rastgele saldırganının veri indirme ve gönderme miktarlarının teşvik modelsiz ve Güven Tabanlı Uyarlanabilir Model ile sonuçlarını göstermektedir. Sonuçlar ortalama bir saldırganın ve iyi niyetli kullanıcının indirdiği ve gönderdiği veri miktarını megabyte olarak göstermektedir. Şekil 18 üzerinde görülebileceği gibi, Güven Tabanlı Uyarlanabilir Model ile birlikte saldırganların indirebildikleri verilerde ufak bir değişiklik olurken iyi niyetli bir kullanıcı ortalama 5GB daha fazla veri indirebilmiş ve gönderebilmiştir.

5.4.2 Bireysel Değişken Bedavacı ve Ayrımcı Bedavacı Saldırganı

Çizelge 8 bireysel değişken bedavacı ve ayrımcı bedavacı saldırganlarının ve iyi kullanıcıların güven tabanlı uyarlanabilir model ile veri gönderme, indirme miktarlarını göstermektedir. Geliştirilen son aşama ile birlikte iyi

Çizelge 8: Bireysel Değişken Bedavacı ve Bireysel Ayrımcı Saldırganlar İle Veri İndirme ve Gönderme Miktarları

	Bireysel Değişken Bedavacı			**Bireysel Ayrımcı Bedavacı**		
	Teşvik Modelsiz	**GT Model**	**GTU Model**	**Teşvik Modelsiz**	**GT Model**	**GTU Model**
Saldırgan Veri Gönderme Miktarı(MB)	4965	1234	2007	3854	426	1061
Saldırgan Veri İndirme Miktarı(MB)	28956	4242	4903	28069	1711	3805
İyi Kullanıcı Veri Gönderme Miktarı(MB)	32132	10087	15088	35010	9579	16153
İyi Kullanıcı Veri İndirme Miktarı(MB)	28419	11250	16532	26847	10801	17840

niyetli kullanıcıların kendilerini sisteme daha hızlı kanıtlamaları, sistemden daha rahat faydalanmaları ve aynı şekilde saldırganların da daha çok etkilenmeleri beklenmekteydi. Sonuçlar üzerinde görülebileceği gibi güven tabanlı modele göre iyi niyetli kullanıcılar ortalama %30-%40 oranında daha fazla veri indirebilmişlerdir ve saldırganlar model tarafından daha fazla cezalandırılarak sistemden daha az faydalanabilmişlerdir. Çizelge 18 üzerindeki veriler Çizelge 5'teki bireysel değişken ve ayrımcı saldırgan verileri ile karşılaştırılabilir. Benzetimde rastgelelik nedeniyle, herhangi bir teşvik modelinin olmadığı durum için aynı sonuçlar elde edilememiştir. İki modelin benzetim sonuçlarına göre iyi kullanıcıların veri indirme ve gönderme miktarında bariz bir artış gözlenmektedir.

5.4.3 İşbirlikçi Saldırganlar İle Deneyler

Çizelge 9: İşbirlikçi Saldırganlar İle Veri İndirme ve Gönderme Miktarları

	Saldırgan Veri Gönderme Miktarı(MB)	**Saldırgan Veri İndirme Miktarı(MB)**	**İyi Kullanıcı Veri Gönderme Miktarı(MB)**	**İyi Kullanıcı Veri İndirme Miktarı(MB)**
Rastgele Bedavacı - Teşvik Modelsiz	3544	27962	29178	28075
Rastgele Bedavacı - GTU Model	1005	4219	16307	13888
Değişken Bedavacı - Teşvik Modelsiz	3735	28613	31658	30455
Değişken Bedavacı - GTU Model	1401	4925	18216	16135
Ayrımcı Bedavacı - Teşvik Modelsiz	4112	28651	30889	28796
Ayrımcı Bedavacı - GTU Model	1097	5149	17969	14410

Çizelge 9 işbirlikçi saldırganların güven tabanlı uyarlanabilir model ile benzetim sonuçlarını göstermektedir. Güven tabanlı uyarlanabilir model işbirlikçi saldırgan benzetimlerinde de iyi niyetli kullanıcılar için daha fazla yarar sağlamıştır. Bu model ile birlikte önceki bölümlerde bahsedildiği gibi iyi niyetli kullanıcılar sistemden daha fazla yararlanabilmişlerken saldırganlar az da olsa daha fazla cezalandırılmışlardır.

5.4.4 Kimlik Değiştiren Saldırgan İle Deneyler

Kimlik değiştirme testi, güven tabanlı uyarlanabilir model bireysel rastgele, bireysel değişken ve bireysel ayrımcı saldırganlar ile günlük hayatta her hafta iki kere kimlik değiştirecek şekilde benzetimi yapılmıştır.

Çizelge 10: Kimlik Değiştiren Saldırgan İle Veri İndirme ve Gönderme Miktarları

	Saldırgan Veri Gönderme Miktarı(MB)	**Saldırgan Veri İndirme Miktarı(MB)**	**İyi Kullanıcı Veri Gönderme Miktarı(MB)**	**İyi Kullanıcı Veri İndirme Miktarı(MB)**
Rastgele Bedavacı - Teşvik Modelsiz	4215	29968	32651	28045
Rastgele Bedavacı - GTU Model	920	7204	13226	10911
Değişken Bedavacı - Teşvik Modelsiz	4806	28634	30999	27915
Değişken Bedavacı - GTU Model	1111	8122	14048	11081
Ayrımcı Bedavacı - Teşvik Modelsiz	4290	29845	35766	30044
Ayrımcı Bedavacı - GTU Model	929	5435	13205	11597

Çizelge 10 kimlik değiştiren saldırganının benzetim sonuçlarını göstermektedir. Model saldırganlar yönünden güven tabanlı model ile benzer sonuçları vermesine rağmen iyi niyetli kullanıcılardaki etkisini bu benzetimde de göstermektedir.

5.4.5 Yüksek Oranda Bedavacı Olan Ağlara İlişkin Deneyler

Bu noktaya kadar yapılan tüm benzetimlerde sistemde %20 oranında kötü niyetli kullanıcı bulunmaktadır. Gerçek hayatta örneğin Gnutella ağında %70'lere varan oranda bedavacı kullanıcılar bulunmaktadır [2]. Bu nedenle güven tabanlı uyarlanabilir modelin yüksek oranda bedavacı içeren durumlardaki başarısını gözlemek amacıyla, saldırganların tüm kullanıcıların %50'sini oluşturduğu ortamların benzetimi bu deneyde yapılmıştır.

Çizelge 11: İşbirlikçi Saldırganlar İle Veri İndirme ve Gönderme Miktarları

	Saldırgan Veri Gönderme Miktarı(MB)	**Saldırgan Veri İndirme Miktarı(MB)**	**İyi Kullanıcı Veri Gönderme Miktarı(MB)**	**İyi Kullanıcı Veri İndirme Miktarı(MB)**
Rastgele Bedavacı - Teşvik Modelsiz	5135	28818	47591	28282
Rastgele Bedavacı - GTU Model	3188	10197	19178	15695
Değişken Bedavacı - Teşvik Modelsiz	5545	29578	48102	29004
Değişken Bedavacı - GTU Model	3820	12011	20982	17839
Ayrımcı Bedavacı - Teşvik Modelsiz	4112	29151	47884	28466
Ayrımcı Bedavacı - GTU Model	3359	11627	20095	16047

Bu bilgiler ışığında Çizelge 11 güven tabanlı uyarlanabilir modelin sistemde %50 saldırgan olduğu durumdaki benzetiminin sonuçlarını

göstermektedir. Sistemde saldırganlar artıkça herhangi bir teşvik modeli olmadığı durumda iyi kullanıcıların veri gönderme miktarlarında çok büyük bir artış gözlenmektedir. Bu durumda saldırganların iyi niyetli kullanıcıları sömürmeleri çok net bir şekilde gözlenmektedir. Güven tabanlı uyarlanabilir modelin uygulanması ile birlikte saldırganların iyi kullanıcıları sömürmeleri engellenmektedir. Benzetimde model ile birlikte iyi kullanıcılar için önceki benzetim sonuçlarına benzer sonuçlar elde edilmiştir. Tüm kullanıcılar kurdukları komşuluklar ve paylaşım oranları ölçüsünde indirme yapabilmişlerdir.

5.4.6 Güven Tabanlı Uyarlanabilir Model İle Deney Sonuçları

Güven tabanlı uyarlanabilir model, güven tabanlı modelde bahsedilen iyi niyetli kullanıcıların fazla etkilenme problemini mümkün olduğunca ortadan kaldırmak için geliştirilmiştir. Modelde, iyi niyetli kullanıcıların mümkün olduğunca kendilerini kanıtlamaları ve sistemden daha fazla yararlanmaları hedeflenmiştir. Benzetim sonuçları güven tabanlı model ile karşılaştırıldığında, iyi niyetli kullanıcılar %20 ile %40 arasında daha fazla veri indirebilmişlerdir.

6 SONUÇ

Eşler arası ağlarda teşvik problemi ele alınması zor ve bir o kadar sistemin sağlığı için gerekli olan bir problemdir. Sistemin gücü paylaşımından geldiği sürece ve sistemde kendi karını maksime etmeye çalışan rasyonel kullanıcılar olduğu sürece teşvik modellerin bulunması kaçınılmazdır. Tez kapsamında güven modeli tabanlı bir teşvik modeli geliştirilmiştir. Geliştirilen model ile güven modellerinin yapılacak geliştirmeler ile birlikte teşvik modeli olarak kullanabileceği gösterilmiştir.

Tez kapsamında geliştirilen model üç aşamada geliştirilmiş ve her bir gelişim aşaması tasarlanan saldırganlar ile benzetimi yapılarak test edilmiştir. Sistemde bireysel olarak hareket eden, işbirliği ile hareket eden ve kimlik değiştirerek hareket eden 3 ana grup altında davranışları farklılık gösteren çeşitli saldırganlar bulunmaktadır. Sistemde toplam 12 farklı saldırgan davranışı bulunmakta olup, modeller bu saldırganlar ile test edilmiştir.

Sistemde ilk olarak paylaşım oranı modeli adı verilen tamamen kullanıcıların indirdikleri ve gönderdikleri veri miktarlarına bağlı olarak bir teşvik sağlamayı amaçlayan bir teşvik modeli geliştirilmiştir. Bu model herhangi bir güven modeli kullanmamaktadır ancak ikinci ve üçüncü aşamalarda temel olan bir modeldir. Bu model kısaca sistemdeki tüm kullanıcıların bant genişliklerine göre bir eşik veri gönderme/veri indirme oranı belirlemekte ve bir kullanıcının dosya indirebilmesi için o andaki paylaşım oranının bu oranın üzerinde olması gerektiğini şart koşmaktadır. Sistemde daha sonra tez kapsamında amaçlanan Güven Tabanlı Model geliştirilmiştir. Bunun için mevcut güven modelleri içerisinde [58] çalışmasındaki güven modeli tercih edilmiştir. Geliştirilen güven tabanlı model ile birlikte bir kullanıcının indirme yapabilmesi için hem paylaşım oranının eşik oran değerinden büyük olması hem de güven değerinin

eşik güven değerinden büyük olması zorunluluğu getirilmiştir. Eşler arası ağlarda bir teşvik modelinin olması, sadece kötü niyetli kullanıcıları değil tüm kullanıcıları etkilemektedir. Sistemdeki tüm kullanıcılar bir teşvik modelinin varlığında kendi davranışlarının iyi olduğunu kanıtlamak zorundadır. Bu kanıtlama evresi aslında modelin sistemdeki kullanıcıları sınama, tanıma evresidir. Bu evre boyunca kullanıcılar, iyi niyetli olsalar dahi sistemden kendi kapasiteleri kadar yararlanamayabilirler. Geliştirilen modelin son aşamasında iyi niyetli kullanıcılar açısından bu evreyi mümkün olduğunca kolaylaştıracak ve kısaltacak geliştirmeler yapılmıştır. Güven Tabanlı Uyarlanabilir Model adı verilen son aşamada kullanıcılara sabit bir eşik oran değeri yerine kullanıcıların davranışına göre tepkiler vererek azalan veya artan uyarlanabilir bir eşik oran değeri sınırlanması getirilmiştir.

Geliştirilen tüm modeller benzetim yardımıyla test edilmiştir. Benzetimde bireysel ve işbirliği davranışı gösteren 8 çeşit bedavacı saldırgan bulunmaktadır. Saldırganlar kendi içerisinde davranışlarına göre ayrılmaktadır. Saldırganlar sisteme çok az veri paylaşmakta veya herhangi bir veri paylaşmamaktadır. Geliştirilen modellerin bu saldırganlar ile benzetimi yapılmış ve modellerdeki beklentiler karşılanmıştır. Paylaşım oranı modeli ile sadece bireysel saldırganlar engellenebilirken, güven tabanlı modellerle tüm saldırganlar engellenebilmiştir.

Kimlik değiştiren saldırgan, teşvik modellerinin baş etmekte en zorlandığı problemlerden biridir. Kullanıcılar sistemde ayrılarak ve yeni bir kimlikle başka bir kullanıcı gibi sisteme tekrar katılarak teşvik modelinin uyguladığı yaptırımlardan kurtulmaya çalışırlar. Son olarak güven tabanlı modeller, gerçek hayatta haftada bir kimlik değiştirecek şekilde ayarlanmış 4 farklı kimlik değiştiren bireysel saldırgan ile test edilmiş ve bu kabuller çerçevesinde bu kullanıcıları engellemeyi başarmıştır.

Geliştirilen model ile ileri aşamalarda daha fazla deney yapılabilir ve model daha da geliştirilebilir. Modelde paylaşım oranı modeli metrikleri

DHT üzerinde tutulmaktadır. Yeni bir saldırgan modeli daha geliştirilerek DHT üzerinde tutulan bu metrikleri değiştirme saldırısı düzenlenebilir. Benzer şekilde modelde her bir kullanıcının başka kullanıcılar hakkında verdiği güven puanı kullanıcının kendisi tarafından saklanmaktadır. Bu metrikler de DHT üzerinde saklanarak buna uygun saldırgan benzetimi gerçekleştirilebilir. Geliştirdiğimiz güven tabanlı modelde kullanıcılar güven değerini mümkünse kendi verdikleri güven puanlarından, mümkün değilse de komşularından gelen tavsiyelere göre hesaplamaktadırlar. Model kapsamında bu hesaplama değiştirilerek tüm kullanıcıların verdiği puanlardan genel veya hibrit bir güven değeri hesaplanabilir. Model kapsamında yapılan benzetimler mümkün olduğunca gerçek bir eşler arası ağ uygulamasına benzer şekilde yapılmıştır. Sistemde bedavacılık oranının belirlenebildiği varsayımı ile bedavacılık oranı belirlenen eşik değerleri geçtiğinde model aktif hale getirilecek şekilde bir benzetim yapılabilir. Ayrıca teşvik modeline makine öğrenmesi yöntemleri eklenerek kendi kendini geliştiren bir güven tabanlı teşvik modeli geliştirilebilir.

Geliştirilen modelin, bir eşler arası ağ uygulamasında kullanılabilir olduğu düşünülmektedir. Bir eşler arası ağ uygulamasında model saldırganların oranından bağımsız olarak ilk aşamadan itibaren kullanılabilir. Model ile birlikte ilk aşamalarda tüm kullanıcılar sınırlamalar ile karşılaşsa dahi kullanıcıların sistem üzerindeki süreleri arttıkça paylaşım yapan kullanıcılar normal davranışlarını sergileyebilmektedirler. Eğer sistemdeki bedavacılık oranı ölçülebiliyor ise, benzer şekilde uygulamanın istediği oran doğrultusunda model sonradan da aktif hale getirilebilir. Böylece modelde eşler ilk aşamalardaki sınırlamalardan kurtulurken, bedavacılık belli bir seviyeye kadar maruz görülebilir.

Sonuç olarak yapılan çalışmalar çerçevesinde güven tabanlı bir teşvik modeli geliştirilmiştir. Benzetim yardımıyla çeşitli saldırganlar ile test edilen bu model başarılı sonuçlar vermiştir. Elde edilen sonuçlar çerçevesinde güven modellerinin yapılacak geliştirmeler ile teşvik modeli olarak da

kullanılabileceği gösterilmiştir.

KAYNAKÇA

[1] J. F. Kurose, *Computer networking: a top-down approach featuring the Internet*. Pearson Education India, 2005.

[2] E. Adar and B. A. Huberman, "Free riding on gnutella," *First Monday*, vol. 5, no. 10, 2000.

[3] Y. Chawathe, S. Ratnasamy, L. Breslau, N. Lanham, and S. Shenker, "Making gnutella-like p2p systems scalable," in *Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications*, pp. 407–418, ACM, 2003.

[4] Clip2, "The gnutella protocol specification v0.4 (document revision 1.2)." http://www.clip2.com/GnutellaProtocol04.pdf, 2001.

[5] A. Kaluszka, "Distributed hash tables," 2010.

[6] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The eigentrust algorithm for reputation management in p2p networks," in *Proceedings of the 12th international conference on World Wide Web*, pp. 640–651, ACM, 2003.

[7] K. Aberer and Z. Despotovic, "Managing trust in a peer-2-peer information system," in *Proceedings of the tenth international conference on Information and knowledge management*, pp. 310–317, ACM, 2001.

[8] L. Xiong and L. Liu, "Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities," *Knowledge and Data Engineering, IEEE Transactions on*, vol. 16, no. 7, pp. 843–857, 2004.

[9] I. Stoica, R. Morris, D. Karger, M. F. Kaashoek, and H. Balakrishnan, "Chord: A scalable peer-to-peer lookup service for internet applications," *ACM SIGCOMM Computer Communication Review*, vol. 31, no. 4, pp. 149–160, 2001.

[10] M. Castro, P. Druschel, A. Ganesh, A. Rowstron, and D. S. Wallach, “Secure routing for structured peer-to-peer overlay networks,” *ACM SIGOPS Operating Systems Review*, vol. 36, no. SI, pp. 299–314, 2002.

[11] B. Y. Zhao, J. Kubiatowicz, A. D. Joseph, *et al.*, “Tapestry: An infrastructure for fault-tolerant wide-area location and routing,” 2001.

[12] S. Ratnasamy, P. Francis, M. Handley, R. Karp, and S. Shenker, *A scalable content-addressable network*, vol. 31. ACM, 2001.

[13] D. Karger, E. Lehman, T. Leighton, M. Levine, D. Lewin, and R. Panigrahy, “Consistent hashing and random trees: Distributed caching protocols for relieving hot spots on the world wide web,” in *In ACM Symposium on Theory of Computing*, pp. 654–663, 1997.

[14] G. Kreitz and F. Niemela, “Spotify–large scale, low latency, p2p music-on-demand streaming,” in *Peer-to-Peer Computing (P2P), 2010 IEEE Tenth International Conference on*, pp. 1–10, IEEE, 2010.

[15] B. Yang and H. Garcia-Molina, “Comparing hybrid peer-to-peer systems,” in *Proceedings of the 27th Intl. Conf. on Very Large Data Bases*, 2001.

[16] D. Artz and Y. Gil, “A survey of trust in computer science and the semantic web,” *Web Semantics: Science, Services and Agents on the World Wide Web*, vol. 5, no. 2, pp. 58–71, 2007.

[17] G. Hardin, “The tragedy of the commons,” *science*, vol. 162, no. 3859, pp. 1243–1248, 1968.

[18] S. Saroiu, P. K. Gummadi, and S. D. Gribble, “Measurement study of peer-to-peer file sharing systems,” in *Electronic Imaging 2002*, pp. 156–170, International Society for Optics and Photonics, 2001.

[19] 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, vol. 24, no. 5, pp. 1010–1019, 2006.

[20] P. Resnick *et al.*, "The social cost of cheap pseudonyms," *Journal of Economics & Management Strategy*, vol. 10, no. 2, pp. 173–199, 2001.

[21] P. Resnick, K. Kuwabara, R. Zeckhauser, and E. Friedman, "Reputation systems," *Communications of the ACM*, vol. 43, no. 12, pp. 45–48, 2000.

[22] J. R. Douceur, "The sybil attack," in *Peer-to-peer Systems*, pp. 251–260, Springer, 2002.

[23] R. Krishnan, M. Smith, and R. Telang, "The economics of peer-to-peer networks," *JITTA*, vol. 5, pp. 31–44, 2004.

[24] G. De Veciana and X. Yang, "Fairness, incentives and performance in peer-to-peer networks," *Seeds*, vol. 250, no. 300, p. 350, 2003.

[25] L. Ramaswamy and L. Liu, "Free riding: A new challenge to peer-to-peer file sharing systems," in *System Sciences, 2003. Proceedings of the 36th Annual Hawaii International Conference on*, pp. 10–pp, IEEE, 2003.

[26] C. Buragohain, D. Agrawal, and S. Suri, "A game theoretic framework for incentives in p2p systems," *arXiv preprint cs/0310039*, 2003.

[27] W. Wu, J. C. Lui, and R. T. Ma, "Incentivizing upload capacity in p2p-vod systems: a game theoretic analysis," in *Game Theory for Networks*, pp. 337–352, Springer, 2012.

[28] R. T. Ma, S. Lee, J. Lui, and D. K. Yau, "Incentive and service differentiation in p2p networks: a game theoretic approach," *IEEE/ACM Transactions on Networking (TON)*, vol. 14, no. 5, pp. 978–991, 2006.

[29] H. Chen, H. Xu, and L. Chen, “Incentive mechanisms for p2p network nodes based on repeated game,” *Journal of Networks*, vol. 7, no. 2, pp. 385–392, 2012.

[30] R. Aumann, “game theory,” in *The New Palgrave Dictionary of Economics* (S. N. Durlauf and L. E. Blume, eds.), Basingstoke: Palgrave Macmillan, 2008.

[31] R. B. Myerson, “Game theory: analysis of conflict,” *Harvard University*, 1991.

[32] R. L. Riolo, M. D. Cohen, and R. Axelrod, “Evolution of cooperation without reciprocity,” *Nature*, vol. 414, no. 6862, pp. 441–443, 2001.

[33] J. F. Nash *et al.*, “Equilibrium points in n-person games,” *Proceedings of the national academy of sciences*, vol. 36, no. 1, pp. 48–49, 1950.

[34] E. Maskin, “Nash equilibrium and welfare optimality*,” *The Review of Economic Studies*, vol. 66, no. 1, pp. 23–38, 1999.

[35] R. B. Myerson, “Refinements of the nash equilibrium concept,” *International journal of game theory*, vol. 7, no. 2, pp. 73–80, 1978.

[36] K. Lai, M. Feldman, I. Stoica, and J. Chuang, “Incentives for cooperation in peer-to-peer networks,” in *Workshop on economics of peer-to-peer systems*, pp. 1243–1248, 2003.

[37] R. M. Axelrod, *The evolution of cooperation*. Basic books, 2006.

[38] H. M. Hochman and J. D. Rodgers, “Pareto optimal redistribution,” *The American Economic Review*, pp. 542–557, 1969.

[39] B. Cohen, “Incentives build robustness in bittorrent,” in *Workshop on Economics of Peer-to-Peer systems*, vol. 6, pp. 68–72, 2003.

[40] S. Jun and M. Ahamad, “Incentives in bittorrent induce free riding,” in *Proceedings of the 2005 ACM SIGCOMM workshop on Economics of peer-to-peer systems*, pp. 116–121, ACM, 2005.

[41] J. Andreoni, “Giving with impure altruism: applications to charity and ricardian equivalence,” *The Journal of Political Economy*, pp. 1447–1458, 1989.

[42] D. Qiu and R. Srikant, “Modeling and performance analysis of bittorrent-like peer-to-peer networks,” in *ACM SIGCOMM Computer Communication Review*, vol. 34, pp. 367–378, ACM, 2004.

[43] L. Guo, S. Chen, Z. Xiao, E. Tan, X. Ding, and X. Zhang, “Measurements, analysis, and modeling of bittorrent-like systems,” in *Proceedings of the 5th ACM SIGCOMM conference on Internet Measurement*, pp. 4–4, USENIX Association, 2005.

[44] M. Piatek, T. Isdal, T. Anderson, A. Krishnamurthy, and A. Venkataramani, “Do incentives build robustness in bittorrent,” in *Proc. of NSDI*, vol. 7, 2007.

[45] K. Walsh and E. G. Sirer, “Experience with an object reputation system for peer-to-peer filesharing,” NSDI, 2006.

[46] D. S. Wallach, P. Druschel, *et al.*, “Enforcing fair sharing of peer-to-peer resources,” in *Peer-to-Peer Systems II*, pp. 149–159, Springer, 2003.

[47] V. Vishnumurthy, S. Chandrakumar, and E. G. Sirer, “Karma: A secure economic framework for peer-to-peer resource sharing,” in *Workshop on Economics of Peer-to-Peer Systems*, vol. 35, 2003.

[48] P. Golle, K. Leyton-Brown, I. Mironov, and M. Lillibridge, “Incentives for sharing in peer-to-peer networks,” in *Electronic Commerce*, pp. 75–87, Springer, 2001.

[49] H. Zhao, X. Yang, and X. Li, “An incentive mechanism to reinforce truthful reports in reputation systems,” *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 951–961, 2012.

[50] W. Dou, H.-M. Wang, Y. Jia, and P. Zou, “A recommendation-based peer-to-peer trust model,” *Journal of software*, vol. 15, no. 4, pp. 571–583, 2004.

[51] L. Xiong and L. Liu, “A reputation-based trust model for peer-to-peer e-commerce communities,” in *E-Commerce, 2003. CEC 2003. IEEE International Conference on*, pp. 275–284, IEEE, 2003.

[52] Z. Liang and W. Shi, “Pet: A personalized trust model with reputation and risk evaluation for p2p resource sharing,” in *System Sciences, 2005. HICSS’05. Proceedings of the 38th Annual Hawaii International Conference on*, pp. 201b–201b, IEEE, 2005.

[53] Z.-g. Shi, J.-w. Liu, and Z.-l. Wang, “Dynamic p2p trust model based on time-window feedback mechanism,” *Journal on Communications*, vol. 31, no. 2, pp. 120–129, 2010.

[54] J.-t. Li, Y.-n. Jing, X.-c. Xiao, X.-p. Wang, and G.-D. Zhang, “A trust model based on similarity-weighted recommendation for p 2 p environments.,” *Ruan Jian Xue Bao(Journal of Software)*, vol. 18, no. 1, pp. 157–167, 2007.

[55] C.-Q. Tian, S.-H. Zou, W.-D. Wang, and S.-D. Cheng, “A new trust model based on recommendation evidence for p2p networks,” *CHINESE JOURNAL OF COMPUTERS-CHINESE EDITION-*, vol. 31, no. 2, p. 270, 2008.

[56] N. Daswani and H. Garcia-Molina, “Query-flood dos attacks in gnutella,” in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pp. 181–192, ACM, 2002.

[57] Y. Tang, H. Wang, and W. Dou, “Trust based incentive in p2p network,” in *E-Commerce Technology for Dynamic E-Business, 2004. IEEE International Conference on*, pp. 302–305, IEEE, 2004.

[58] A. B. Can and B. Bhargava, “Sort: A self-organizing trust model for peer-to-peer systems,” *IEEE Trans. Dependable Sec. Comput.*, vol. 10, no. 1, pp. 14–27, 2013.

[59] S. Saroiu, K. P. Gummadi, and S. D. Gribble, “A Measurement Study of Peer-to-Peer File Sharing Systems,” in *Multimedia Computing and Networking (MMCN)*, January 2002.

[60] S. Saroiu, K. P. Gummadi, R. J. Dunn, S. D. Gribble, and H. M. Levy, “An analysis of internet content delivery systems,” 2002.

[61] A. B. Can, *Trust and Anonymity in Peer-to-peer Systems*. PhD thesis, West Lafayette, IN, USA, 2007.

ÖZGEÇMİŞ

Kimlik Bilgileri

Adı Soyadı	:	Serkan ÇAKMAK
Doğum Yeri	:	Ankara
Medeni Hali	:	Bekar
E-Posta	:	serkancakmak89@gmail.com
Adresi	:	Eryaman Mah. Etimesgut/Ankara

Eğitim

Lise	:	Polis Koleji (2003-2007)
Lisans	:	Hacettepe Üniversitesi Bilgisayar Mühendisliği Bölümü (2007-2011)

Yabancı Dil ve Düzeyi

İngilizce - ileri

İş Deneyimi

2011-2013 Milsoft A.Ş. - Yazılım Mühendisi

2013-2014 Türkiye İstatistik Kurumu - Yazılım Mühendisi

Deneyim Alanları

Java, C, C++, C#, Assembly, UML, SQL, Office araçları, Doors, JSF
Enterprise Architect, Windows OS, Linux (Ubuntu),
MS-DOS, MS Visual Studio 6.0/2005/2008/2010, Eclipse, NetBeans

Tezden Üretilmiş Projeler ve Bütçesi

-

Tezden Üretilmiş Yayınlar

-

Tezden Üretilmiş Tebliğ ve/veya Poster Sunumu İle Katıldığı Toplantılar

Tebliğ : Eşler Arası Ağlarda Teşvik Modelleri
(Incentive Models in Peer-to-peer Networks)

Yer : IscTurkey2013 - 6. Uluslararası Bilgi Güvenliği
ve Kriptoloji Konferansı, Türkiye - 2013