ÜST-N LİSTESİ ÜRETEN ÖNERİ SİSTEMLERİNİN SEGMENT ATAĞA KARŞI GÜRBÜZLÜĞÜNÜN ANALİZİ

Yüksek Lisans Tezi

Ayşe YAZICI

Eskişehir 2019

ÜST-N LİSTESİ ÜRETEN ÖNERİ SİSTEMLERİNİN SEGMENT ATAĞA KARŞI GÜRBÜZLÜĞÜNÜN ANALİZİ

Ayşe YAZICI

YÜKSEK LİSANS TEZİ

Bilgisayar Mühendisliği Anabilim Dalı

Danışman: Doç. Dr. Cihan KALELİ

Eskişehir

Eskişehir Teknik Üniversitesi

Lisansüstü Eğitim Enstitüsü

Kasım 2019

JÜRİ VE ENSTİTÜ ONAYI

Ayşe YAZICI'nın "Üst-N Listesi Üreten Öneri Sistemlerinin Segment Atağa Karşı Gürbüzlüğünün Analizi" başlıklı tezi ..... tarihinde aşağıdaki jüri tarafından değerlendirilerek "Eskişehir Teknik Üniversitesi Lisansüstü Eğitim-Öğretim ve Sınav Yönetmeliği'nin ilgili maddeleri uyarınca, Bilgisayar Mühendisliği Anabilim dalında Yüksek Lisans tezi olarak kabul edilmiştir.

Jüri Üyeleri	**Unvanı Adı Soyadı**	**İmza**
Üye (Tez Danışmanı)	: Doç. Dr. Cihan KALELİ	……
Üye	: Doç. Dr. Alper Kürşat UYSAL	……
Üye	: Dr. Öğr. Üyesi Efnan Şora GÜNAL	……

Prof. Dr. Murat TANIŞLI
Lisansüstü Eğitim Enstitüsü Müdürü

ÖZET

ÜST-N LİSTESİ ÜRETEN ÖNERİ SİSTEMLERİNİN SEGMENT ATAĞA KARŞI GÜRBÜZLÜĞÜNÜN ANALİZİ

Ayşe YAZICI

Bilgisayar Mühendisliği Anabilim Dalı

Bilgisayar Bilimleri Bilim Dalı

Eskişehir Teknik Üniversitesi, Lisansüstü Eğitim Enstitüsü, Kasım 2019

Danışman: Doç. Dr. Cihan KALELİ

Üst-N listesi üreten öneri sistemleri, internet dünyasında etkili bir şekilde kullanılan iş birlikçi filtreleme(İF) yöntemidir. Bu sistemler kullanıcının ilgilenebileceği, henüz satın almadığı ürünlerin listesini önerirken, benzer kullanıcılar veya benzer ürünler üzerinden çeşitli algoritmalar aracılığı ile tahminde bulunurlar. Belirli bir alana yönelimi görülen kullanıcı için yine o alana uyan önerilerde bulunmak sistemi başarılı kılabilir. Öneri sistemleri kullanıcıların hareketlerinden yola çıkarak topladıkları bilgiyi kullanırlar ve bu yol sistemleri bazı kötü amaçlı saldırılara açık hale getirir. Literatürde şilin atak ismiyle anılan saldırılar, sistemin kararlılığını bozar ve öneri sistemlerinin başarısını düşürür.

Bu tez kapsamında, üst-N listesi üreten öneri sistemi belirli bir kategori üzerine uygulanmıştır. Saldırı çeşitlerinden biri olan Segment Atak yapılarak sistemin kararlılığı incelenmiştir. Yapılan deneyler ile atağın başarılı olup olmadığı, üst-N öneri sisteminin atak yapılmadan önceki ve sonraki başarı oranları karşılaştırılmıştır.

Anahtar Sözcükler: Üst-N Öneri Sistemleri, Şilin Atak, Gürbüzlük Analizi

ABSTRACT

ROBUSTNESS ANALYSIS OF TOP-N RECOMMENDATION SYSTEMS AGAINST SEGMENT ATTACK

Ayşe YAZICI

Department of Computer Engineering

Program in Computer Sciences

Eskişehir Technical University, Institute of Graduate Programs, November 2019

Supervisor: Assoc.Prof.Dr. Cihan KALELİ

Recommendation systems that produce the top-N list are collaborative filtering(CF) method that is used effectively in the Internet World. These systems suggest a list of products that the user may be interested in, not yet purchased, while using similar users or similar products to predict them through various algorithms. For a user who is oriented to a specific area, making recommendations that match that area can make the system successful. Recommendation systems use the information based on collect from the users' inputs, which makes these systems vulnerable to some malicious attacks. In the literature, these type of attacks named as shilling attacks, disrupt the stability of the system and reduce the success of recommendation systems.

Under this thesis, the recommendation system which produces a top-N list has been applied on a specific category. The stability of the system is examined by conducting a Segment Attack, which is one of the types of Shilling Attacks. The success rates of the top-N recommendation system were compared with the experiments conducted before and after the attack.

Keywords: Top-N Recommendation Systems, Shilling Attacks, Robustness Analysis

TEŞEKKÜR

Çalışmalarım süresince bilgi ve deneyimleriyle bana yol gösteren, değerli tez danışmanım Sayın Doç. Dr. Cihan Kaleli'ye teşekkürlerimi sunarım. Tez sunumumda jüri üyeleri olarak yer alan Sayın Doç. Dr. Alper Kürşat Uysal ve Sayın Dr. Öğr. Üyesi Efnan Şora Günal'a çalışmam konusundaki düzeltmeleri ve yapıcı yorumlarından dolayı teşekkürlerimi sunarım.

Tez süresince yanımda olan desteklerini her daim yanımda hissettiğim sevgili aileme ve sevgili eşime teşekkürlerimi sunarım.

Ayşe YAZICI
Kasım,2019

11/11/2019

ETİK İLKE VE KURALLARA UYGUNLUK BEYANNAMESİ

Bu tezin bana ait, özgün bir çalışma olduğunu; çalışmamın hazırlık, veri toplama, analiz ve bilgilerin sunumu olmak üzere tüm aşamalarında bilimsel etik ilke ve kurallara uygun davrandığımı; bu çalışma kapsamında elde edilen tüm veri ve bilgiler için kaynak gösterdiğimi ve bu kaynaklara kaynakçada yer verdiğimi; bu çalışmanın Eskişehir Teknik Üniversitesi tarafından kullanılan "bilimsel intihal tespit programı"yla tarandığını ve hiçbir şekilde "intihal içermediğini" beyan ederim. Herhangi bir zamanda, çalışmamla ilgili yaptığım bu beyana aykırı bir durumun saptanması durumunda, ortaya çıkacak tüm ahlaki ve hukuki sonuçları kabul ettiğimi bildiririm.

Ayşe YAZICI

İÇİNDEKİLER

ŞEKİLLER DİZİNİ

TABLOLAR DİZİNİ

SİMGELER VE KISALTMALAR DİZİNİ

***a*:** Aktif kullanıcı

İF: İş birlikçi filtreleme

***k*:** Komşuluk sayısı

N: Önerilecek ürün sayısı

RMSE: Ortalama hata kareleri toplamı kökü

1. GİRİŞ

Öneri sistemleri günümüzde birçok şirket tarafından satışlarını ve kârlarını artırmak amacıyla gerekli görülen bir sistem haline gelmiştir (Güneş ve ark., 2014). Kullanıcıların görüşlerini, tercihlerini önemseyen bu sistemler internet dünyasındaki bilgileri filtreleyerek kişiye özel öneriler sunarlar. Önerileri büyük bilgi dünyasından çekerek doğru öneriyi müşteriye sunabilmek büyük şirketler için yüksek önem taşır. Bu nedenle de öneri sistemlerinin geliştirilmesi, iyileştirilmesi konusunda yapılan çalışmalar geçmişten günümüze dek sürmektedir.

Bir öneri sistemi kişiye en doğru öneriyi yapmak amacıyla veri madenciliği yöntemlerini kullanarak ürünler hakkında tahminler üretir. Bu tahminlerin doğruluğu kullanıcının sisteme güveni açısından büyük önem taşır. Öneri sistemleri kullanıcının devasa bilgi yığınından kendisine uygun ürünleri çekip ayırmasını sağlar. Kullanıcının sistemden bir ürün için istediği öneriye tahmin adı verilir. Öneri sistemleri her bir ürün için kişiye özgü farklı tahminler üretir. Bu tahminlerden yola çıkarak kişi ürünü sevip sevmeyeceğine karar vererek, ürünü satın alma eğiliminde bulunabilir. Bu nedenle yapılan tahminlerin doğruluğu satıcıların kâr oranlarıyla doğru orantılıdır. Öneri sistemlerinin diğer bir kullanım şeklinde ise, kullanıcı sistemden kendine en uygun ürünleri listelemesini isteyebilir. Bu durumda birden fazla ürün için tahminler üretilerek, bu tahminler büyükten küçüğe doğru sıralanarak beğeni sırasına göre kullanıcıya sunulur. Kullanıcının beğenebileceği N adet ürünün sistemden çekilerek kişiye özgü üretilen öneri listelerine üst-N listesi adı verilir. Üst-N listesinde kullanıcının sevebileceği ürünler, en çok beğenebileceği ürün ilk sırada olacak şekilde sıralanır. Kişiye daha çok öneri yapıldığı için deneyimleyebileceği ürün sayısı çoğalır. Bu durum kişinin önerilen ürünleri sevme ihtimalini artarak sistemin doğru öneri yapma oranını arttırır. Tüm bu özelliklerinden dolayı, üst-N listesi üreten öneri sistemleri popüler şirketler tarafından tercih edilen etkileyici bir öneri üretme yöntemidir.

Öneri sistemleri gerçek kullanıcıların gerçek deneyimlerinden yola çıkarak öneriler ürettikleri için zararlı saldırılara açıktırlar. Sisteme dahil olan her kullanıcı gerçek olmayabilir. Sahte kullanıcıların öneri sistemlerini kendi yararları uğruna manipüle ederek sisteme dahil olmasıyla gerçekleştirilen zararlı yazılımlara şilin atak denir. Rakip şirketler birbirlerinin ürünlerinin popülaritesini azaltmak ya da arttırmak amacıyla öneri sistemlerine şilin atak gerçekleştirebilirler. Bu saldırılar sonucunda

gerçek olmayan kullanıcılar öneriye dahil edildiğinden, sistemin ürettiği öneriler doğruluğunu kaybeder. Sistemdeki kullanıcı sayısı kalitesiz bir şekilde çoğaldığından sistemin cevap verme süresi uzar, kararlılığını kaybeder. Zamanla iyice gelişen ataklar, sistem hakkında bilgi edinmeden dahi sisteme zarar verebilecek hale gelmiştir. Bu ataklarla mücadele etmek öneri sistemlerinin karşılaştığı çetin zorluklardandır.

Tez kapsamında, öneri sistemlerinin en yoğun kullanılan yöntemlerinden biri olan üst-N listesi çalışılmıştır. Kullanıcı tabanlı öneri sistemi geliştirilerek sistemdeki kullanıcılar üzerinden belirli bir segmente ait filmleri izleyen kişilere üst-N listesi oluşturulmuştur. Geliştirilen öneri sisteminin başarısını ölçmek amacıyla test metodolojileri uygulanmıştır. Şilin atak türlerinden biri olan segment atak tipinde sahte kullanıcılar oluşturularak sistemin ataklara karşı tepkisi ölçülmüştür.

Bu çalışmanın amacı, başarılı öneriler üreten üst-N öneri sisteminin bir kategori alanındaki başarısınının değerlendirilmesi ve bununla birlikte belirli bir segment üzerinde zararlı değişiklik yapmak isteyen segment atak türüne karşı sistemin gücünün ölçülmesidir. Öneri sistemi aynı zamanda büyük kullanıcı ve ürün kümesine sahip olan veri kümesi üzerinde de test edilerek algoritmanın başarısı ölçülmüştür.

Tez çalışmasının devamında toplam beş bölüm içerisinde izlenen yol ve yapılan deneyler akış sırasına göre sıralanmıştır.

Çalışmanın ikinci bölümünde, literatürde öneri sistemleriyle ilgili yapılan çalışmalar incelenmiştir. Üst-N listesi üreten öneri sistemleri, şilin ataklar ve gürbüzlük analizi konularında günümüze kadar yapılan çalışmalar sıralanmıştır.

Üçüncü bölümde, çalışmada incelenen deneyleri ve amaçları anlayabilmek adına teorik ön bilgiler bölümü yer almaktadır. İş birlikçi filtreleme(İF) yöntemi ve şilin atakların genel tanımı ile alandaki kullanım biçimleri formüller ile birlikte anlatılmaktadır.

Dördüncü bölümde, üst-N listesi oluşturma aşamaları ile çalışmada kullanılan veri setinde yer alan kategori bilgileri bulunabilir. Kullanılan veri setlerinin özellikleri ile yapılan deneylerin aşamaları ve sonuçlarının yer aldığı bilgiler bu bölümde açıklanmıştır.

Zararlı saldırıların tanımlandığı, atak çeşitlerinden biri olan segment atağın yapısı ve işleyişi beşinci bölümde anlatılmıştır. Bu atak özelinde sistemin nasıl etkilendiği, bu bölümün deney sonuçları kısmında incelenmiştir.

Altıncı bölümde, sonuçların yorumlanması ve bu çalışmanın sağladığı katkılardan bahsedilmiştir. Gelecek çalışmalar için bu alanda yapılabilecek işler not edilmiştir.

2. LİTERATÜR

Öneri sistemleri çalışma alanı, yıllar içerisinde giderek ihtiyaç duyulan bir sistem haline gelmesinden ve sürekli gelişiminden dolayı araştırmalara yön vermektedir. İF öneri sistemleri hakkında süregelen çalışmalar içinde üst-N listesi üreten öneri sistemleri alanında da oldukça önemli çalışmalar yapılarak literatüre yeni yöntemler ve yaklaşımlar katılmıştır. Şilin ataklar olarak bilinen kötü amaçlı saldırılar, öneri sistemlerinin uzun zamandır yeni çözümler bulmaya çalıştığı bir mücadele konusudur. Şilin atakların tespiti, yapısının tanınması ile ilgili çalışmalar bu alandaki popüler çalışmalardandır.

Tez kapsamında ele alınan üst-N öneri sistemlerinin zararlı girişimlere karşı sistemin gürbüzlüğünün ölçülmesi konusunda yapılan çalışmalar yetersizdir. İF yöntemlerinin gürbüzlüğünün incelenmesi birçok çalışmada yer alırken İF tabanlı üst-N öneri sistemleri özelinde bir çalışmaya rastlanmamıştır.

Literatürde anlatılan çalışmalara göre, öneri sistemlerinin bir çeşidi olan üst-N öneri sistemlerinin şilin atağa karşı gürbüzlüğünün incelenmesi bu tez çalışmasında yapılan bir yeniliktir. Tez çalışmasının bu bölümde anlatılan çalışmalardan farkı, üst-N listesi üreten öneri sistemleri özelinde segment atağın sisteme etkisinin deneylerle incelenmesidir.

Bu bölümde, tez kapsamında ele aldığımız üst-N listesi üreten öneri sistemleri ve yapılan ataklara karşı sistemin gürbüzlüğünün ölçülmesi ile bağlantılı olarak sırasıyla üst-N öneri sistemleri, şilin ataklar ve öneri sistemlerinin gürbüzlük analizi hakkında yapılan çalışmalar yer almaktadır.

2.1 Üst-N Öneri Sistemleri

Öneri sistemlerinin popüler uygulamalarından biri olan bu yöntem, tüketiciye büyük bir ürün kümesinden, N adet ürünün seçilip önerilmesidir (P.Cremonasi, 2010). İF, oldukça yaygın kullanılan bir üst-N öneri yöntemidir (J.Herlocker, 2002; J.Lee, 2012). İF yöntemi, kullanıcı ürün değerlendirmeleri veya çevrimiçi gezintilerden aldığı bilgiler gibi kişi özelinde topladığı bilgilerle ilgilenir (B.Kanagal, 2012). Bu yöntem geçmişte ortak bir değerlendirmede birleşmiş kullanıcıların gelecekte de ortak bir değerlendirme yapabilecekleri üzerine kuruludur.

İF tabanlı üst-N öneri sistemlerinin oluşturulmasında iki önemli yaklaşım bulunur. İlk yaklaşıma göre; her kullanıcı mutlaka benzer zevklere sahip geniş bir kullanıcı kümesiyle bağdaşır (Shardanand ve Maes, 1995; Konstan ve ark. 1997; Breese ve ark. 1998; Resnick ve ark. 1994; Herlocker ve ark. 1999; Sarwar ve ark. 2000). *Kullanıcı bazlı* olan bu yaklaşımdan dolayı, o kümeye ait kullanıcılar için öneri yapılırken gruptaki diğer kullanıcıların ürünler ile etkileşimlerinin kullanılması doğru bir yaklaşımdır. İkinci yaklaşım olan *model bazlı* yaklaşıma göre; bir ürün ya da ürünlerin alınması, diğer ürün ya da ürünlerin alınmasına neden oluyorsa, bu ürünler arasında ilişki olduğunu gösterir. Ürünlerin arasındaki ilişki, sistem tarafından öneri oluşturulurken kullanılır (Shardanand ve Maes, 1995; Billsus ve Pazzani 1998; Breese ve ark. 1998; Aggarwal ve ark. 1999; Kitts ve ark. 2000). Model bazlı yaklaşımda, ürünler arasındaki ilişki çevrimdışı hesaplandığı için önerinin üretilme süresinde ciddi bir kazanım olur. Bu modelin dezavantajı, modeli oluşturmak için gerekli zaman ve gereksinimdir. Ayrıca, kullanıcı bazlı yaklaşımlar daha kaliteli önerilerde bulunurken, ürün bazlı önerilerde doğruluk ölçütünden bir miktar taviz verilir. Kullanıcı bazlı sistemlerde ise kullanıcı sayısı arttığında sistemin öneri üretme süresi uzar. Netflix gibi milyonlarca kullanıcının yer aldığı bir platform düşünüldüğünde, kullanıcı bazlı hesaplamalar dezavantajlı olur.

Deshpande ve Karypis(2004), üst-N öneri sistemleri hakkında çalışmalar yapan ve problemi tanıtan ilk araştırmacılardandır. Sarwar (2001) ın ürün bazlı İF sistemi çalışmasını, ürünlerin benzerliğinin bulunması aşamasına iki yeni yöntem katarak genişletmişlerdir. İlk yöntemde ürünler kullanıcı uzayında bir vektör olarak düşünülmüştür ve kosinüs benzerliği formülü ile hesaplanarak ürünler arasındaki benzerlik çıkartılmıştır. Diğer yöntemde ise iki ürün arasındaki benzerlik, koşullu olasılık tekniğiyle hesaplanmıştır.

Karypis(2001) çalışmasında üst-N listesi üreten ürün bazlı İF sistemleri hakkında çalışmış ve yeni değerlendirme ölçütlerini tanıtmıştır. Bu model de diğer ürün bazlı modellerdeki gibi soğuk başlatma(cold start) problemlerine takılmıştır.

Kim(2007) kullanıcı bazlı İF sisteminde, kullanıcılardan gelen dönüşe göre bir hata matrisi oluşturmuş, gerçek puan ve tahmin edilen puan arasındaki fark hata matrisine kaydedilerek, ortalama hata değerine göre tahmin yapılmıştır. Bu yöntem de

kullanıcıların ve ürünlerin yeterli miktarda bulunmadığı boşluklu matrise sahip öneri sistemlerinde başarı gösterememiştir.

McLaughlin(2004) kullanıcı bazlı üst-N öneri listesi üren İF metodu kullanarak İnanmaDağılımı(BeliefDistribution) algoritmasını tanımlamıştır. Bu algoritmada inanma(dağılım) değeri oylama değişimlerine bakarak hesaplanmıştır. Her kullanıcının ortalama oy değeri ile ürünler için tahmin edilen oy değerinin farkını inanma farkı(belief difference) olarak tanımlamışlardır.

Christakopoulou(2018) çalışmasında, evrensellikle kullanıcı alt kümesine özgü gizli faktörler kümesini birleştirip, iki yeni görünmez uzay modellemesini tanıtmışlardır.

Nikolakopoulos(2019) üst-N öneri sistemleri için ürün-ürün grafikleri üzerinde kişiselleştirilmiş dağılımı, yapay sinir ağlarıyla öğrenmeye çalışarak yeni bir sistem geliştirmiştir.

2.2 Şilin Ataklar

İF metodu ile öneri yapılırken kullanıcı özelinde öneri sunabilmek için veri kullanıcılardan direkt ya da dolaylı olarak toplanır. Bu durum aslında yapılan önerilerin kişiye özgü olmasını sağlayarak başarıyı getirse de başarısızlığın yolunu açabilecek zararlı girişimlere de yol gösterir. Profil enjeksiyonu ve şilin ataklar denilen bu durumlar İF algoritmalarının en büyük zayıflığı olarak tanımlanırlar (O'Mahony ve ark., 2002; Burke ve ark., 2006b).

Şirketler, kendi avantajları için kullanıcı ürün değerlendirmelerine müdahale edip sahte kullanıcılar ekleyerek kendi ürünlerini ön plana çıkarmak ya da rakip firmanın ürünlerinin satışlarını aşağıya çekmek isteyerek sistemin performansını düşürmek isteyebilirler (O'Mahony ve ark., 2002). Örneğin bir şirket kendi ürünlerininin satışlarını arttırmak için ürünlerine yüksek oy veren gerçek olmayan kullanıcıları sisteme dahil edebilir. Aynı şekilde rakip firmanın ürünlerine düşük oy veren sahte kullanıcıları sisteme dahil edebilir. Bu durumda sistemde kullanıcı sayısı arttığı için yavaşlama olurken, sahte kullanıcılardan kaliteli bilgi toplanmadığı için yapılan önerilerin kalitesi de düşer. Bu sebeplerden dolayı ilgili ataklara anında müdahale edilmesi zorunlu hale gelmiştir (Burke ve ark., 2005a).

Şilin ataklar üzerinde çalışmalar yapan araştırmacılar, yaptıkları çalışmaları dört ana grupta toplarlar (Güneş ve ark., 2014). Sahte profil enjekte ederek İF sistemlerine saldıran şilin atakları oluşturmak, sistemde yer alan atakları tespit etme yöntemleri, ataklara karşı güçlü duracak algoritmaların geliştirilmesi ve ataklara karşı sistemlerin gürbüzlüğünün ölçülmesi bu alanda yapılan ana çalışmalardır. Bu tezde yapılan çalışmalar ise, üçüncü ve dördüncü ana başlıkta yapılan çalışmaların konusu altına girmektedir.

2.2.1 Şilin atak oluşturma stratejileri ve profil enjeksiyonu

İF sistemlerine dışarıdan kötü niyetlerle sahte profiller ekleyip öneri sistemlerinin kararlarının etkilenebileceği ilk defa O'Mahony (2002) tarafından ortaya konulmuştur. Sonraki çalışmalarında ise öneri sistemi hakkında yeterli bilgiye sahip olunmasa bile atakların başarılı şekilde gerçekleştirilebileceğini kanıtlamıştır (O'Mahony ve ark., 2005).

Lam ve Riedl (2004, 2005) *rasgele(random)* ve *ortalama(average)* atak tipini tanıtmışlardır. Şilin atakların ne kadar etkili olabilecekleri üzerine araştırmalar yapmışlardır. Burke ve ark. (2005d) güvenli İF sistemleri kurabilmek için gerekli ana maddeleri ortaya koymuştur. *Tutarlılık(Consistency), bölüm(segmented), sürü(bandwagon)* atak tiplerini tanıtmıştır. Ayrıca diğer çalışmasında, Burke ve ark. (2005a) *Sürü* ve *popüler ürün(popüler item)* atak tiplerinin başarısını ölçmüştür. Burke ve ark. (2005b,c) çalışmasında ortak bir kategoride benzer zevkleri olan kullanıcıları hedef alan *segment* atak tipini önermiştir. *Ters sürü(Reverse bandwagon)* ve *sevme/nefret(love/hate)* atak tipleri Mobasher ve ark. (2007b) tarafından, hedef ürünün düşmesini hedefleyen nuke atak tipi olarak tanıtmıştır. Hafıza (memory) tabanlı atak tipleri alanındaki çalışmaların haricinde model tabanlı atak tipleri de çalışılmıştır.

Cheng ve Hurley (2009) model bazlı sistemleri hedef alan *çeşitli(diverse)* ve *gizlenmiş(obfuscated)* atak tiplerini tanıtmışlardır. *Kopyalanmış ürün enjeksiyon (Copied-item injection)* atağı ise Oostendorp ve Sami (2009) tarafından tanıtılmıştır, ün bazlı öneri sistemlerini hedef alır.

2.2.2 Şilin atakları tespit etme çalışmaları

Kirli bilginin sisteme girmesi ve öneri sisteminin güvenilirliğini etkilemesi ile bu atakların tespiti için çalışmalar yapılması kaçınılmaz hale gelmiştir. Popüler bir alan

olan atak tespit çalışmaları *denetimli(supervised), denetimsiz(unsupervised)* ve *yarı-denetimli(semi-supervised)* tekniklerine göre gruplandırılmıştır.

Atakların tespiti yapılırken, (Burke ve ark. 2006a,b; Chirita ve ark. 2005; Mobasher ve ark., 2006b) gibi daha bir çok isim problemi sınıflandırma yöntemlerini kullanarak çözmeye çalışmışlardır. Bu çalışmalar denetimli teknikler kullanılarak yürütülmüştür.

Denetimsiz tekniklerin kullanıldığı çalışmalardan örnek verirsek; O'Mahony (2004) kümeleme yöntemi ile komşuluk seçerek, Su ve ark. (2005) benzerlik yayılması algoritmasını tanıtarak atakların bulunmasına yardımcı olan çalışmalar yapmışlardır.

Zhou(2018) anormal kullanıcı grubu bulgularına ve oylama zaman aralıklarına bakarak şilin atak tespit yapısı oluşturmuştur. Şüpheli oylamaları tespit edebilmek için şüpheli zamanda pencere ve hedef ürün analizi yöntemini kullanmışlardır.

Yakın zamanlarda ise SriKanth ve Shashi(2019) zararlı kullanıcıların ve atak hedefi olan ürünün tespiti için Rating Deviation from Mean Bias (Ortalama Eğilim Oylama Sapması (RDMB)) ve Compromised Item Deviation(Anlaşılmış Ürün Sapması (CID)) isimli iki yeni metrik önermişlerdir. RDMB atak kullanıcılarını tespit ederken, CID hedef ürünün tespiti için geliştirilmiştir.

Atak tespiti ile ilgili detaylı çalışmaların bilgisi Burcu Yılmazel(2016) doktora çalışmasında bulunabilir.

2.2.3 Ataklara karşı güçlü algoritmaların geliştirilmesi

Araştırmacılar ataklara karşı koyacak güçlü sistemler için dayanıklı algoritma geliştirme üzerine çalışmalar yapmışlardır. Bu alanda yapılan çalışmalara, akıllı komşuluk seçme algoritması çalışması, O'Mahony ve ark. (2004b,c), etki limitleyici algoritmasıyla Resnick ve Sami (2007), doğrusal ve asimptotik olarak doğrusal algoritmalarıyla Van Roy ve Yan (2009,2010) örnek olarak verilebilir. Konu hakkındaki daha detaylı bilgi ataklara karşı güçlü algoritmaları analiz eden (Mehta ve Hofmann, 2008; Güneş ve ark., 2014; Burke ve ark., 2015; Aggarwal, 2016a) çalışmalarında bulunabilir.

2.2.4 Kullanılan algoritmaların gürbüzlük analizi

Sistemin performansını ölçmek amacıyla ilk kez O' Mahony ve ark. (2002) çalışmasında bahsedilmiştir. Burke ve ark. (2005a) ve Mobasher ve ark. (2005) çalışmalarında kullanıcı ve ürün bazlı öneri sistemleri için atakların etkilerini araştırmıştır.

İkili değer, yani 1 ve 0 şeklindeki veriyle çalışan öneri sistemlerinin gürbüzlük analizi çalışmaları da yapılmıştır. Long ve Hu (2010) kullanıcı bazlı öneri sistemlerinde numerik ve ikili değer verilerinin gürbüzlüğünü karşılaştırmış, ikili değer kullanan öneri sisteminin ataklara dayanıklılığının daha fazla olduğu tespit edilmiştir. Kaleli ve Polat(2013) , çalışmalarında ikili değerler kullanan sistemlerin gürbüzlüğünü ölçmek için *oran değişimi(ratio shift)* denilen yeni bir metrik geliştirmişlerdir.

Turk ve Bilge (2019) çalışmasında temel sayılabilecek çok kriterli öneri üretme algoritmalarının şilin ataklara karşı gürbüzlüğünü incelemişlerdir. Bu tür çok kriterli sistemlere yapılabilecek genel bilinen şilin atakların genişletilip bu sisteme uygun hale getiren yeni atak şemaları üzerinde çalışmışlardır.

Çalışmamızda ele alınan üst-N öneri sistemlerinin gürbüzlük analizine dair araştırmalar bu konuda çalışma bulunmadığından dolayı, özgün bir çalışma konusu sayılabilir.

3. ÖN BİLGİLER

3.1 İş Birlikçi Filtreleme Yöntemi

Öneri sistemlerinin kullandığı pek çok yöntemden en popüleri olan İF yöntemi, kullanıcıların geçmişte bir ürün hakkında ortak zevke sahip olmalarının, gelecekte de bir ürün hakkında ortak görüşte birleşebilecekleri üzerine kuruludur. Kullanıcı bazlı İF sistemlerinde kullanıcıların ortak zevkleri üzerinden benzer kullanıcılar bulunurken, ürün bazlı İF sistemlerinde ürünlerin kullanıcılar tarafından birlikte alımıyla benzerlik tanımlanır. Her iki yöntem için de en benzer kullanıcı veya ürün üzerinden çeşitli algoritmalar kullanılarak sistemden öneri isteyen aktif kullanıcıya(a) öneri hesaplanır.

Öneri sistemleri gerçek kullanıcıların gerçek ürünler hakkında gerçek değerlendirmeleri üzerinden yola çıkarak öneri üretir. Kullanıcıların değerlendirmeleri iki yolla toplanır. Birincisi, kullanıcıların bir ürün hakkında sisteme görüş bildirmesi aracılığıyla olur. Örneğin; bir filmi oylamak veya bir ürünü beğen düğmesine basmak gibi kişisel görüşler doğrudan sisteme aktarılır. İkinci yol ise kullanıcının bir siteyi ziyaret etmesi, bir sayfada uzun süre kalması gibi dolaylı olarak görüşlerin sisteme aktarılmasıdır. İki yolda da kullanıcıların ürünler hakkındaki görüşleri yeni bir kullanıcıya veya henüz deneyimlemediği ürün hakkında öneri isteyen kullanıcıya öneri üretmek amacıyla kullanılır.

Kullanıcıların değerlendirmelerini tutmak amacıyla bir n*m boyutlu matris oluşturulur. n satır kullanıcının m sütun ürün üzerinde değerlendirmelerinden oluşan bu matris öneri sistemi için bir girdi olur. 1-5 arasındaki oy değerlerini puanlama olarak kullanan bir sistemin kullanıcı ürün değerlendirme matris örneğini Tablo 1.1de görebiliriz. Tabloya bakarak birinci kullanıcının üçüncü ürünü beğendiğini, birinci ürünü henüz deneyimlemediğini, ikinci kullanıcının ise birinci ürünü beğenmediğini, ikinci ürünü ise deneyimlemediği söylenebilir.

Tablo 3.1 *Kullanıcı-ürün değerlendirme matrisi*

	Ürün1	Ürün2	Ürün3	....	...	...	ÜrünM
Kullanıcı1	0	3	5				0
Kullanıcı2	1	0	2				1
....	...	...	...				...
KullanıcıN	0	0	5				2

Kullanıcıların görüşleri elimizde olduğundan, bir ürün hakkında sistemden öneri isteyen *a* kullanıcısının, diğer kullanıcılar ile benzerliği çeşitli benzerlik hesaplarıyla hesaplanır. Bunlardan en sık kullanılan aşağıda formülü gösterilen Pearson Korelasyon Katsayısı benzerlik hesabıdır (Resnick ve ark., 1994).

$$w(a,i) = \frac{\sum_j (v_{a,j} - \overline{v_a})(v_{i,j} - \overline{v_i})}{\sqrt{\sum_j (v_{a,j} - \overline{v_a})^2 \sum_j (v_{i,j} - \overline{v_i})^2}} \quad (3.1)$$

*a'*ya en benzer komşu sayısı (*k)* kadar kullanıcı öneri üretmek üzere seçilir. Seçilen komşular yakınlık ağırlıklarına göre öneri hesabına katkıda bulunurlar. En benzer kullanıcının puan tahminine en büyük katkıyı sağladığı söylenebilir. Öneri hesabı için yaygın kullanılan aşağıdaki formülle *a'* nın j ürününe vereceği puan tahmin edilir (Breese ve ark. 1998).

$$p_{a,j} = \overline{v_a} + k \sum_{i=1}^{n} w(a,i) \left(v_{i,j} - \overline{v_i}\right) \quad (3.2)$$

k tane komşunun aktif ürüne verdiği puanlar üzerinden yapılan hesaplamaya göre *a'*ya öneri üretilir. Yapılan önerinin doğruluğu öneri sistemleri açısından çok önemlidir. Önerinin doğruluğunu arttırmak için yapılan çalışmalar, kullanıcıların güveninin kazanılmasını sağlar. Bu sebeple araştırmacılar birçok benzerlik hesabı yöntemi ve öneri üretme algoritmaları üzerinde çalışmıştır.

Üst-N listesi üreten öneri sistemlerinde, *a* kullanıcısına birden fazla ürün hakkında hesaplanan tahminler, büyükten küçüğe doğru sıralanır. Böylelikle *a* 'nın sevebileceği birden fazla ürün beğeni sırasına göre sıralanmış şekilde kullanıcıya önerilmiş olur. Sıralanmış ürünlerden ilk N tane ürün seçildiğinde oluşan listeye üst-N öneri listesi adı verilir. Bir ürün önerisi yerine birden fazla ürünün önerilmesi kullanıcının herhangi bir ürünü sevme ihtimalini arttırır, dolayısıyla sisteme güvenilirliği arttırıcı etkenlerdendir.

3.2 Şilin Atak

Öneri sistemleri kaynak olarak kullanıcıların görüşlerini kullandıklarından bazı kötü amaçlı saldırılara ve bilginin kalitesizleştirilmesine açıktırlar. Öneri sistemlerinde şilin atak veya profil enjeksiyon saldırıları ismiyle anılan bu yazılımlar sisteme dahil olarak sistemin kararsız hale gelmesine neden olurlar. Amaçlarına ve tiplerine göre

farklılaşarak birçok çeşidi bulunan şilin ataklar genel olarak bir ürünün popülaritesini arttırmak veya azaltmak amacıyla hareket ederler.

İF sistemlerine kendilerini ekleyerek kullanıcı-ürün matrisine dahil olan kötü niyetli kullanıcılar veya firmalar, sistemi manipüle ederek yapılan öneriyi kalitesizleştirirler. Şirketler kendi ürünlerinin satışlarını arttırmak amacıyla öneri sistemlerine ürünlerinin puanını yükselten sahte kullanıcılar eklerler. Rakip firmaların ürünlerinin popülaritesini azaltmak için rakip ürünlere düşük puanlar veren sahte kullanıcıları sisteme dahil ederler. Bir ürünü ön plana çıkarmak için yapılan ataklar *itme(push)* atağı olarak adlandırılırken, ürünün popülaritesini düşürmek amacıyla yapılan ataklar *çekme(nuke)* atağı olarak tanımlanır.

Şilin atak yapılırken oluşturulan sahte kullanıcıların genel profili Şekil 3.1 deki gibidir (A. Bilge,2016).

I_S	I_F	I_O	I_T
S ürün: Atak karakteristiğini belirler	F ürün: Atak tespitini zorlaştırır	O ürün: Değerlendirme sunulmamış ürün	Hedef ürün

Şekil 3.1 *Sahte kullanıcı genel profili*

I_s bölümünde yer alan ürünler atağın karakteristiğini belirleyen ürünlerdir. Bu kısım için seçilen ürünlere göre atağın hangi tipte yapıldığı dışarıdan okunabilir. I_f kısmında atağın dışarıdan görünürlüğünü azaltmak, sistemdeki diğer kullanıcılara benzemesini sağlayarak farkedilmesini engellemek amacıyla doldurulan ürünler yer alır. I_o kısmında ise değerlendirilmemiş ürünler yer alır. I_t ise popülaritesini dışarıdan müdahale ederek yükseltmeye veya alçaltmaya çalışılan hedef ürünü simgeler. Şilin atak yapılan bir sistemde, hedef ürün kullanıcılara önerildiyse ve bir itme atağı yapıldıysa atak başarılı olmuştur. Eğer çekme şilin atağı yapıldıysa ve ürün artık kullanıcılara önerilmiyorsa başarılı bir atak yapılmıştır.

Bir öneri sisteminde kullanıcıların ürünler üzerindeki değerlendirmeleri bir matris aracılığıyla tutulur. Tablo 3.1 de görüldüğü gibi kullanıcılar satırları, ürünler ise sütunları oluştururken değerler kullanıcıların puanlamalarından oluşur. Bu şekilde bilgi toplanan sistemlerde, her internet kullanıcısı en az bir ürünü değerlendirerek sisteme

dahil olabilir. Bu nedenle kötü amaçlı yazılımlar ile sisteme sahte kullanıcılar kolaylıkla eklenebilir.

Tablo 3.2 *Sahte kullanıcıların sisteme eklenmesi*

	Ürün1	Ürün2	Ürün3	....	Hedef Ürün	...	ÜrünM
Kullanıcı1	0	3	5		0		0
Kullanıcı2	1	0	2				1
....	...	...	...				...
KullanıcıN	0	0	5				2
SahteKullanıcı1	0	1	1		5		0
SahteKullanıcı2	1	0	1		5		1
...	0	0	0		5		0
SahteKullanıcı_s	0	0	1		5		1

Sahte kullanıcıların her biri gerçek bir kullanıcı gibi öneri sistemine eklenir. Tablo 3.2 de görüldüğü gibi s adet sahte kullanıcı öneri sistemine eklendiğinde direkt olarak kullanıcı ürün matrisine yazılır. Bu durumdan dolayı gerçek kullanıcılara üretilen önerilerin doğruluğu azalır. Tabloda eklenen sahte kullanıcıların hedef ürüne en yüksek oyu temsil eden 5 puanı vererek itme atağı gerçekleştirildiği görülebiliyor. Eklenen sahte profiller, bazı filmlere 1 puan vererek ve bazılarını ise oylamayarak gerçek kullanıcılarla benzerlik yakalamayı ve farkedilmemeyi sağlamaya çalışıyorlar. Dışarıdan bakan biri bu durumdan dolayı hangi profilin sahte hangisinin gerçek olduğunu tespit edemeyebilir. Birçok araştırmacı bu konuyu inceleyerek şilin ataklarının tespiti üzerine çalışmalar gerçekleştirmişlerdir.

Öneri sisteminin kararsızlaşmasıyla, gerçek bir kullanıcı sisteme dahil olduğunda daha önce kullanıcıya önerilmeyecek olan hedef ürün artık bu kişiye önerilebilir. Kullanıcı önerilen ürünü sevmediğinde ise sisteme güveni azalabilir ve başka firmaların ürünlerine yönelebilirler. Sahte kullanıcılar sistemdeki aktif kullanıcı sayısını arttırdığından öneri üretilirken harcanacak zaman artabilir, bu durum gerçek veriye sahip kullanıcıların sabırsızlaşmasına yol açabilir.

4. BELİRLİ SEGMENT ÜZERİNE ÜST-N LİSTESİ OLUŞTURULMASI

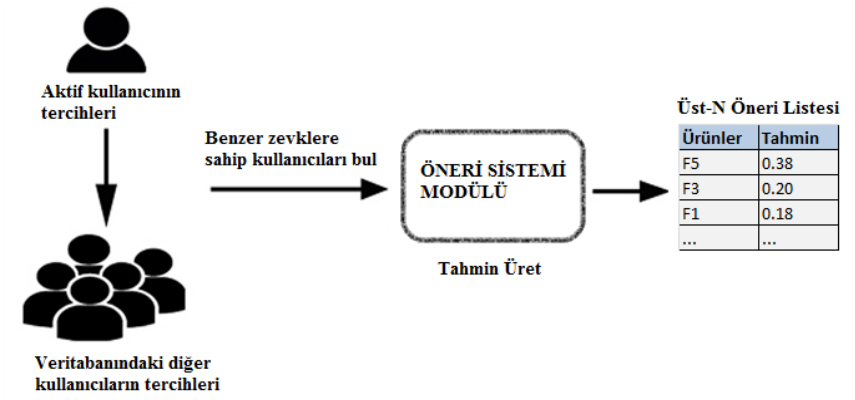
Öneri sistemleri büyük bir bilgi havuzunun bulunduğu internet ortamında ürünleri önerirken, kullanıcıların tercihlerini göz önünde bulundurarak kişi bazlı öneride bulunmayı amaçlarlar. Yapılacak önerinin kişiyle bağdaşması, müşterinin güvenini kazanmaya, alışverişlerinin artmasına ve dolayısıyla şirketlerin kârının artmasına fayda sağlayacaktır.

Bu sistemler kullanıcıya tek bir ürün veya onun zevkine en uygun N tane ürün listesi önerebilirler. Bu tez kapsamında kişinin sevebilme ihtimali yüksek en uygun ürünlerin listesini içeren üst-N listesi adı verilen yazılım geliştirilmiştir. İlerleyen bölümlerde, üst-N listesinin nasıl oluşturulduğu, veri kümesindeki kategori bilgilerinin sunulması ve algoritmanın işleyişi ile sistemin başarısının nasıl test edildiği anlatılmaktadır.

4.1 Üst-N Listesi Tanımı

Öneri sistemlerinde en etkili kullanılan yöntem İF yöntemidir. Bu yöntem kullanıcı bazlı ve ürün bazlı filtreleme olarak iki şekilde uygulanabilir. Kullanıcı bazlı yöntemde temel varsayım eskiden benzer ürünleri beğenen kullanıcılar yeni deneyimleyecekleri ürünlerde de benzer zevkleri paylaşabilirler. Ürün bazlı filtreleme metodunda ise ürünlerin birlikte alınması başka bir ürünün daha alınmasını doğuruyor olabileceği varsayımından yola çıkılır.

İF algoritmaları toplamda üç aşamadan oluşur. İlk aşamada; kullanıcıların ürünler hakkındaki görüşleri toplanır. Bu bilgiler kullanıcıdan aldığı ürünü oylaması gibi direkt olarak alınabilir veya bir siteyi ziyaret etmesi, bir ürünü incelemesi baz alınarak dolaylı olarak toplanabilir. İkinci aşama; kullanıcılar veya ürünler arasındaki benzerliği hesaplama aşamasıdır. Kullanıcı bazlı benzerlik hesapları yapılırken genellikle Pearson Korelasyon Katsayısı kullanılır (Resnick ve ark., 1994). Bu katsayı formülü kullanılarak *a* ile diğer kullanıcıların birlikte oyladıkları ürünlerde ne kadar benzedikleri bilgisi ağırlık verisi olarak tutulur. Son aşama ise önerinin hesaplanması aşamasıdır. Bu aşamada; *a* ile en benzer *k* tane kullanıcının oyları benzerlik oranları hesaba katılarak belirli katsayılar ve normalizasyon işlemleri sonucunda *a'* nın hedef ürüne vereceği oy değeri tahmin edilir.



Şekil 4.1 *Genel bir üst-N öneri sistemi şeması*

Üst-N listesi üretilirken yukarıda bahsedilen tüm aşamalar gerçekleştirilirken, sadece son aşamada bir farklılıktan söz edilebilir. Bir ürün için tahmin oluşturmak yerine henüz kullanıcının deneyimlemediği tüm ürünler için tahmin üretilir. Bunların arasından N tane en yüksek tahmine sahip ürün *a*' ya önerilir.

4.2 Kategori Verisinin Toplanması

Tez kapsamında yapılan deneylerde veri seti olarak MovieLens 100K veri seti kullanılmıştır. GroupLens araştırma projesi kapsamında Minnesota Üniversitesinde toplanan bu veri, 943 kullanıcının 1682 film üzerine verdikleri 100.000 oydan oluşmaktadır. Oy değerleri; 1 puan en düşük oyu, 5 puan ise en yüksek oyu temsil edecek şekilde 1 ile 5 arasındaki tam sayılardan oluşmaktadır.

MovieLens verisinde yer alan 1682 filmin hangi kategoriye girdiği GroupLens tarafından yayınlanan *u.item* metin dosyasından edinilebilmektedir. Komedi dalındaki 505 adet filmin ve drama dalındaki 725 adet filmin kimlikleri buradan belirlenmiştir.

4.3 Üst-N Listesi Oluşturulması

Gerçekleştirilecek deneylerde kullanılmak üzere, MovieLens verisinden 700 adet kullanıcı deneme, 243 adet kullanıcı test için kullanılmak üzere rastgele seçilmiştir. Test kullanıcılarından her biri için sadece ilgili segmente ait oy değerleri dikkate alınarak, kullanıcının oy vermediği filmlerin bilgisi çıkartılmıştır.

Öneri üretilirken, benzerlik hesabında en çok kullanılan yöntemlerden biri olan *k-nn* en yakın komşuluk yöntemi uygulanmıştır. Bu yöntem ile her bir test kullanıcısının, tüm deneme kullanıcılarıyla benzerliği Pearson formülü ile hesaplanmıştır. En yüksek

ağırlık değeri, *a* ile o değere sahip deneme kullanıcısının en benzer olduğu anlamına gelir. Daha sonra bu değerler büyükten küçüğe sıralanarak ilk *k* tanesi seçilir. Öneri üretilirken kullanılacak en yakın komşular böylelikle belirlenmiş olur.

Önerilerin üretileceği ürün setlerini belirlerken ise, her bir test kullanıcısının o kategorideki filme oy verip vermediği bilgisi tutulmuştur. Bu nedenle her test kullanıcısı için ürün seti farklılaşabilmektedir. Örneğin; bir test kullanıcısının izlediği komedi filmleri ile birlikte izlemediği komedi filmlerinin bilgisi de bulunmaktadır. Kullanıcının izlemediği tüm komedi filmleri için bu filmlere ait bir tahmin oluşturulacaktır. Buradaki varsayım daha önce komedi filmi izlemiş birisi yine bu alandaki filmleri tercih edebilir üzerinedir.

Son aşama ise her bir test kullanıcısı için önerilerin yapıldığı aşamadır. Test kümesinde yer alan *a'* nın belirli kategorideki oylamadığı tespit edilen filmlere, en yakın komşularının o filmler için verdikleri oylar hesaba katılarak tahmini oy değerleri oluşturulur. Bu tahmini değerler büyükten küçüğe doğru sıralanırken, değerin büyüklüğü değil, hangi filme ait olduğu bilgisi bizim için önemlidir. Kullanıcının en çok beğenebileceği tahmin edilen filmler, en yüksek tahminin üretildiği filmlerdir. En yüksek tahminden en düşük tahmine doğru sıralanan filmler listesinden N tane seçilerek üst-N listesi oluşturulur.

Algoritmanın sözde kodunda bahsedilen tüm aşamalar sırasıyla gösterilmiştir.

Algoritma 1 Üst-N listesi oluşturma algoritması

girdi: Kullanıcı-ürün matrisi (test ve deneme verisi olarak rastgele ayrılmış); *Deneme, Test*

Öneri için kullanılacak en yakın komşu sayısı; *k*

Segmente ait filmlerin kimlikleri; *segmentürünleri*

Önerilecek ürün sayısı; *N*

çıktı: Üst-N öneri listesi; *üst-N*

Listenin dışında kalan ürünler; *atak*

u: test kullanıcısı

x: deneme kullanıcısı

i: film

M: öneri matrisi

1: foreach u ∈ Test **do**

2: Z(u,i) ← oy vermediği segment filmlerini bul

3: ağırlık(u,x) ← tüm deneme kullanıcılarıyla olan benzerliğini hesapla *(3.1)*

4: [Y,I] ← azalaraksırala(ağırlık(u,x))

5: I(1,1:k) ← en yakın *k* tane komşuyu seç *(k-nn algoritması)*

6: Result(u,i) ← Z(u,i) ye öneri üret *(3.2)*

7: M(u,i)← azalaraksırala(Result(u,i))

8: üst-N(u,1:N)← ilk N adet i yi seç

9: atak(u,:) ← üst-N(u,1:N) dışında kalan filmler

10:end

11:döndür üst-N,atak

Test kullanıcılarının her biri için yukarıdaki işlemler uygulanır. Her bir test kullanıcısı için oluşturulan üst-N listeleri saklanırken, listenin dışında kalıp tahmin oluşturulmuş filmler başka bir listede tutulur. Bu listeler ileriki kısımlarda açıklayacağımız atak deneyleri için kullanılacaktır.

4.4 Test Metodolojisi

Öneri sistemlerinde kullanıcılara ürünleri önermenin yeterli olacağı düşünülse de, önerinin doğru yapılıp yapılmadığını ölçmek için bir takım metrikler geliştirilmiştir. İF öneri algoritmalarında sıkça kullanılan RMSE metriği üst-N listeleri için bir ölçüt değildir. RMSE metriği tahmin edilen değer ve gerçek değer arasındaki farka

odaklanırken, üst-N listesi üretirken hesaplanacak hata ürünlere verilen oy değerlerinin farkından değil, ürünlerin listeye hangi sırayla girdiği veya girip girmediği ile ilgilenir. Bu tez kapsamında, üst-N listesi üreten öneri sistemlerinin başarısını ölçmek için *duyarlılık* ve *kesinlik* ölçütleri kullanılmıştır.

Bu bölümde; kullanılan veri setleri tanıtılmış, algoritmanın performansını ölçmek için kullanılan yöntem adımları anlatılmıştır. Duyarlılık ve kesinlik ölçme metrikleriyle algoritmanın başarı hesabı yapılarak bölüm sonlandırılmıştır.

4.4.1 Kullanılan veri setleri

Üst-N listesi üreten algoritmanın başarılı öneriler üretebildiğini test etmek amacıyla iki farklı veri seti üzerinde çalışılmıştır. Birinci veri seti birçok akademik çalışmada kullanılan MovieLens veri seti iken, diğer veri seti milyonlarca veriden oluşan Netflixin yayınladığı kullanıcı-film-oy değerlendirmelerinden oluşan Netflix Prize veri setidir.

Netflix 2006 yılında kendi öneri algoritmasının hata oranınından daha düşük bir algoritma geliştirebileceğini düşünen adaylar için bir yarışma düzenlemiştir. Bu yarışma için kullanılacak veri setini sitesinde yayınlamıştır. Netflix Prize veri seti, 4 parçadan oluşan kullanıcı-film-oy değerlerinden oluşan *deneme* seti ve *probe* adı verilen yapılacak önerilerin doğruluğunu test edecek verileri içermektedir.

İki veri setinin özellikleri aşağıdaki tabloda gösterilmektedir.

Tablo 4.1 *Veri setlerinin istatiksel bilgileri*

Veri Seti	Kullanıcı Sayısı	Film Sayısı	Oy Sayısı
MovieLens	943	1682	100K
Netflix Prize	480189	17770	100M

4.4.2 Duyarlılık ve kesinlik hesabının yapılması

Tez kapsamında geliştirilen üst-N öneri sisteminin başarısını test etme yöntemi Paolo, Yehuda ve Roberto (2010) yılındaki çalışmalarında yapılan yönteme benzemektedir.

Kullanılan veri setine göre uygulanan yöntem adımları farklılaşabilmektedir. Verilerin test ve deneme kümesi olarak ayrılma yöntemi, kategori alanında öneri yapılıp yapılmamasına bağlı olarak test basamakları değişiklik gösterebilir.

MovieLens veri seti için uygulanan yöntem sırasıyla 5 adımdan oluşur.

1. Veri rastgele deneme kullanıcıları ve test kullanıcıları kümelerine ayrılır.
2. Her test kullanıcısının, kategoriye ait filmlerden en yüksek oyu (5 puan) verdiği ürünler belirlenir. Bu filmlerin kullanıcı tarafından beğenilmesinin kesinliğinden yola çıkılır.
3. Test kullanıcısının sevdiği belirlenen her bir ürün ve kullanıcı tarafından henüz oylanmamış kategoriye ait filmler için öneri üretilir.
4. Öneri üretilmiş bütün filmler sıralanır ve ilk N tanesi seçilir. Eğer kullanıcının sevdiği film bu listenin içindeyse doğru bir öneri yapılmıştır. Yapılan öneri *isabetli* olmuştur. İlgili ürün kullanıcıya önerilmediyse ise *ıskalama* durumu olmuştur.
5. Kullanıcının oylanmamış kategori filmlerinin sayısı ve sevdiği bir ürün sayısı kadar öneri listeye alınacağında, her zaman *isabetli* öneri yapılır. N değeri arttıkça *isabetli* önerilerin sayıları da artar.

Netflix veri seti için uygulanan yöntem sırasıyla aşağıdaki basamaklardan oluşur. MovieLens veri setinde izlenen adımlardan bazı yönleriyle farklılaşsa da aynı yolu izledikleri söylenebilir.

1. Deneme kümesi ve probe kümesi Netflix tarafından ayrı dosyalar ile paylaşılmıştır. Test kümesi, probe kümesinde yer alan kullanıcı ve filmlerden, herhangi bir filme 5 puan vermiş kullanıcılardan seçilip oluşturulmuştur. Test kullanıcıları deneme kümesinde de yer aldıkları için buradan çıkartılmıştır.
2. Her test kullanıcısının, tüm filmlerden en yüksek oyu (5 puan) verdiği ürünler belirlenir. Bu filmlerin kullanıcı tarafından beğenilmesinin kesinliğinden yola çıkılır.
3. Test kullanıcısının sevdiği belirlenen her bir ürün ve kullanıcı tarafından henüz oylanmamış 1000 film rastgele seçilir ve her biri için öneri üretilir. Kullanıcının bu filmleri sevmeyeceği tahmin edilerek yola çıkılır.

4. Öneri üretilmiş bütün filmler sıralanır ve ilk N tanesi seçilir. Eğer kullanıcının sevdiği film bu listenin içindeyse doğru bir öneri yapılmıştır. Yapılan öneri *isabetli* olmuştur. İlgili ürün kullanıcıya önerilmediyse ise *ıskalama* durumu olmuştur.
5. Kullanıcının oylanmamış 1000 filmi ve sevdiği bir ürün sayısı kadar öneri listeye alınacağında (N=1001), her zaman *isabetli* öneri yapılır. N değeri arttıkça *isabetli* önerilerin sayıları da artar.

Her bir test basamağı, bir test kullanıcısının 5 puan verdiği filmlere teker teker öneri üretilip, üst-N listesine girip giremediğinin test edilmesinden oluşur. Tüm test kullanıcıları bitene kadar devam eder. Bu basamaklarda oluşan her *isabet* kümülatif olarak toplanır ve toplam *isabet* sayısı elde edilir. Test kullanıcılarının 5 puan verdiği filmlerin sayısı da kümülatif toplanarak işlem sayısı elde edilir. *Duyarlılık* ve *kesinlik* değerleri aşağıdaki formüller ile hesaplanır.

$$duyarlılık(N) = \frac{\#\text{isabet}}{|\text{T}|}$$

$$kesinlik(N) = \frac{\#\text{isabet}}{\text{N}.\ |\text{T}|} = \frac{\text{duyarlılık(N)}}{\text{N}}$$

|T| : test kullanıcılarının 5 puan verdiği tüm filmlerin sayısı

#isabet: tüm test kullanıcılarına yapılan önerilerin kümülatif isabet sayısı

N: En yüksek önerilerden kaç tanesinin listeye alınacağı bilgisi

4.5 Deneyler ve Sonuçları

Gerçekleştirilen deneylerde iki farklı veride algoritmanın başarı oranını ölçmek amacıyla MovieLens ve Netflix Prize veri setleri kullanılmıştır. İki veri seti de kullanıcı-film değerlendirmelerinden oluşmaktadır. MovieLens küçük bir kullanıcı ve ürün veri kümesini temsil ederken, Netflix ise geniş bir kullanıcı ürün veri kümesini temsil eder.

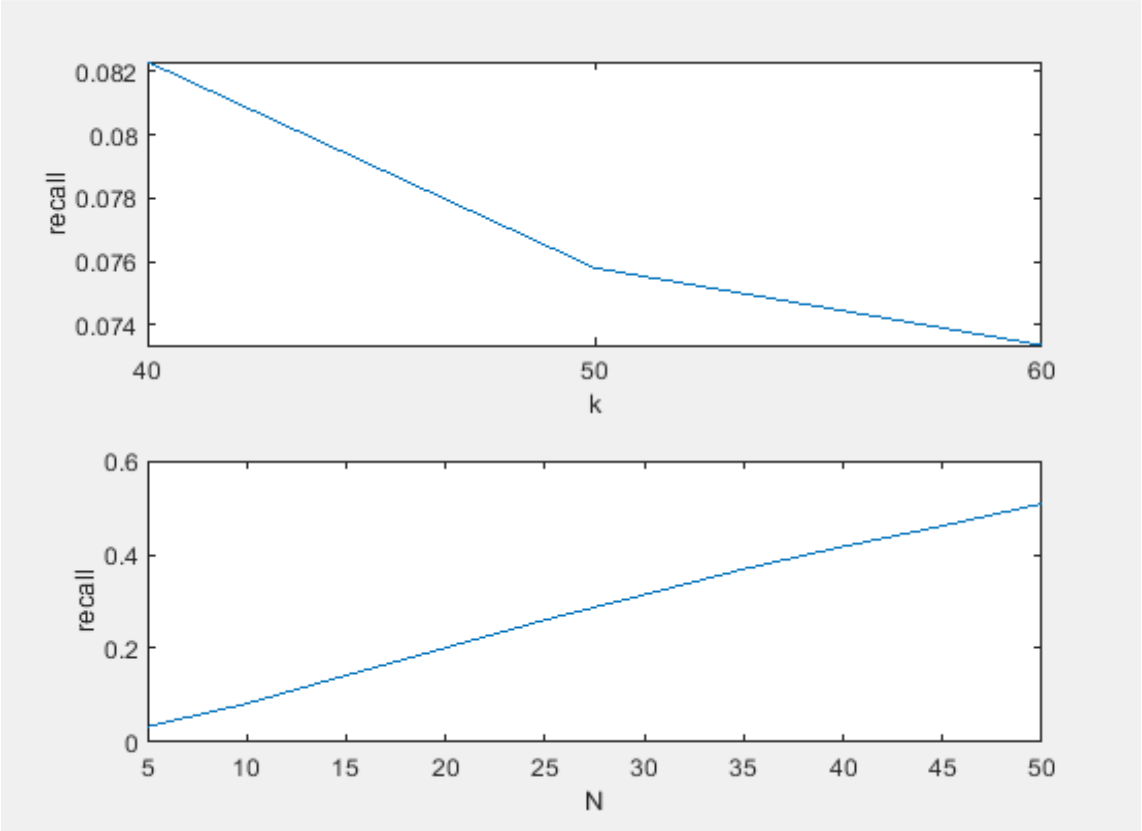
Deneylerde *k* ve N parametreleri değiştirilerek duyarlılık değerinin nasıl etkilendiği ölçülmektedir. Duyarlılık değerinin yüksek olması algoritmanın kalitesini gösterir.

İlk deneyde önerilecek filmlerin sayısını gösteren N, 10 değerine sabitlenmiştir. Komşuluk sayısının değişimiyle sistemin hassasiyetinin değişimi gözlenir. *a'* ya en yakın komşularından kaç tanesinin algoritma tarafından öneri üretmek için kullanılacağını *k* değeri gösterir. Deneyin bu kısmında bir kullanıcıya 10 tane film önerilirken, *k* parametresi 40, 50 ve 60 parametrelerine göre test edilmiştir. Şekillerde birinci grafik ile gösterilmektedir.

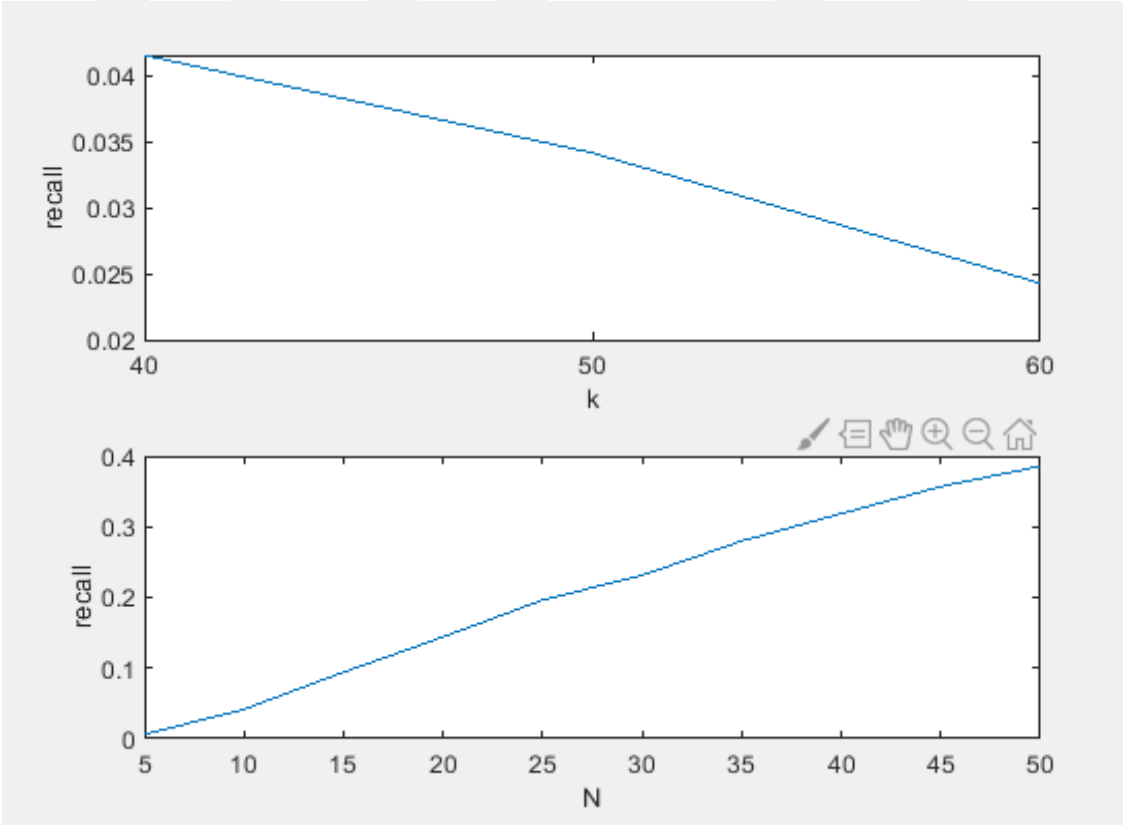
İkinci deneyde ise önerilecek ürünlerin sayısının artmasıyla sistemin hassasiyetinin değişimi gözlenmiştir. *a' ya* en yakın 40 komşu seçilerek *k* değeri sabitlenmiştir. N değerine ise [5,10,...,45,50] parametreleri verilerek duyarlılığın değişimi hesaplanmıştır. Şekillerde ikinci grafik ile gösterilmektedir.

4.5.1 MovieLens deney sonuçları

MovieLens verisi üzerinde iki farklı kategori üzerinde çalıştırılmıştır. MovieLens verisindeki komedi ve drama kategorilerine ait filmlerin oylamaları dikkate alınmıştır. İki kategorideki deney sonuçları grafiklerde gösterilmiştir.



Şekil 4.2 *k ve N parametrelerine göre duyarlılık(recall) değişimi-MovieLens(komedi kategorisi)*

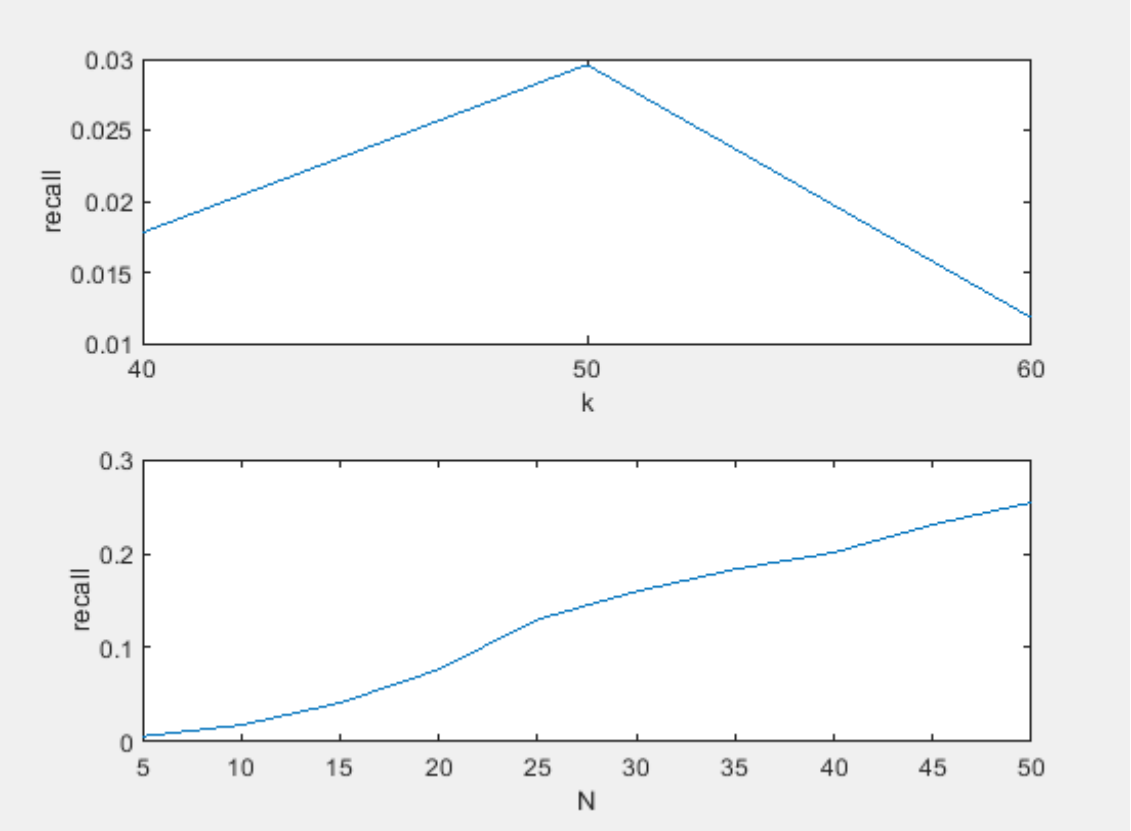


Şekil 4.3 *k ve N parametrelerine göre duyarlılık(recall) değişimi-MovieLens(drama kategorisi)*

Grafikler incelendiğinde iki kategori için de parametrelere göre duyarlılığın aynı yönde değişim gösterdiği görülmektedir. İki kategoride de komşuluk sayısının artmasıyla başarının düştüğü, önerilecek ürün sayısının fazlalaşmasıyla ise başarının arttığı görülmektedir. Kategorideki film sayısı arttığında ise sistemin duyarlılığının azaldığı gözlemlenmektedir. Daha çok filme sahip drama kategorisindeki duyarlılığın, aynı parametrelere bakıldığında, görece daha az filme sahip komedi kategorisinin duyarlılığından daha az olduğu görülmektedir.

4.5.2 Netflix deney sonuçları

Netflix Prize tarafından yayınlanan deneme kümesi orijinal haliyle deneye dahil edilmiştir. Probe setinde yer alan kullanıcılardan, 5 puan verdikleri filmler dikkate alınarak seçilen kullanıcılar ise test kümesini oluşturur. Test kümesinden ilk 100 test kullanıcısı seçilerek deneyler için kullanılmıştır.



Şekil 4.4 *k ve N parametrelerine göre duyarlılık(recall) değişimi-Netflix*

Grafik incelendiğinde, en yakın komşulardan seçilen sayı arttıkça, yönelimin iki yönde de ilerlediğini söyleyebiliriz. Komşu sayısı ilk arttığında öneriye olumlu yönde katkı olmasına rağmen, daha fazla komşu algoritmaya dahil edildiğinde önerinin başarısının düştüğü görülmektedir. N parametresinin artmasıyla ise yapılan önerinin daha başarılı hale geldiği görülüyor.

5. ÜST-N ÖNERİ SİSTEMLERİNE ŞİLİN ATAK YAPILMASI

İnternet üzerinden alışveriş yıllar geçtikçe popüler hale geldiğinden, büyük şirketler öneri sistemlerinde kullandıkları algoritmaları dolayısıyla sistemlerini geliştirmeye çalışmaktadırlar. Kullanıcılara doğru tahminler yaptıkça, şirketler müşterilerinin güvenini kazanır. Müşteriye sevebileceği ürünü önerip, sonuçtan müşterinin de memnun kaldığı durumlar ne kadar çok oluşursa şirketler kârlarını ve güvenilirliklerini o kadar arttırırlar. Aksi durumda, memnun kalmayan müşteriler alternatif siteleri deneyebilirler Güneş (2013b).

Toplanan veri kullanıcılardan direkt (oy verme vb.) ya da dolaylı (web sitesini ziyaret vb.) olarak alınabilir. Kullanıcıdan alınan veri öneri sistemlerinin girdisini oluşturduğu için yüksek kalitede olması çok önemlidir. Verinin yüksek kalitede olması demek, gerçek kullanıcılardan ve gerçek kullanıcıların gerçek değerlendirmelerinden oluşması demektir. Çevrimiçi alışveriş şirketleri kendi ürünlerini ön plana çıkartmak, rakip firmalara zarar ettirmek için bazı yollara başvururlar. Bunlara genel olarak bilgisayar dünyasında şilin atak adı verilir. Bu ataklar, gerçekte var olmayan kullanıcılar oluşturarak belirli ürünleri ön plana çıkartırlar ve sistemin kararlılığını bozarlar. Kalitesiz verinin içeriye girmesi ve kullanıcı sayısının fazlalaşması öneri sisteminin uzun sürede tahmin üretmesine ve doğru karar verememesine neden olur.

Ataklar genel olarak amaçlarına ve bilgi gereksinimlerine göre gruplandırılırlar Mobasher (2007a). Bir atak eğer bir veya birden fazla ürünün ön plana çıkması amacıyla yapılıyorsa *itme (push) atağı*, eğer ürünün veya ürünlerin popülerliğini düşürmek amacıyla yapılıyorsa *çekme (nuke) atağı* diye isimlendirilir. Bilgi gereksinimlerine göre ataklar; *düşük bilgi (low knowledge)* ve *yüksek bilgi (high knowledge)* gerektirenler olarak ikiye ayrılırlar. Yaygın olarak kullanılan, bilgi ihtiyacı düşük itme ataklarından biri olan segment atak bu tez kapsamında ele alınmıştır.

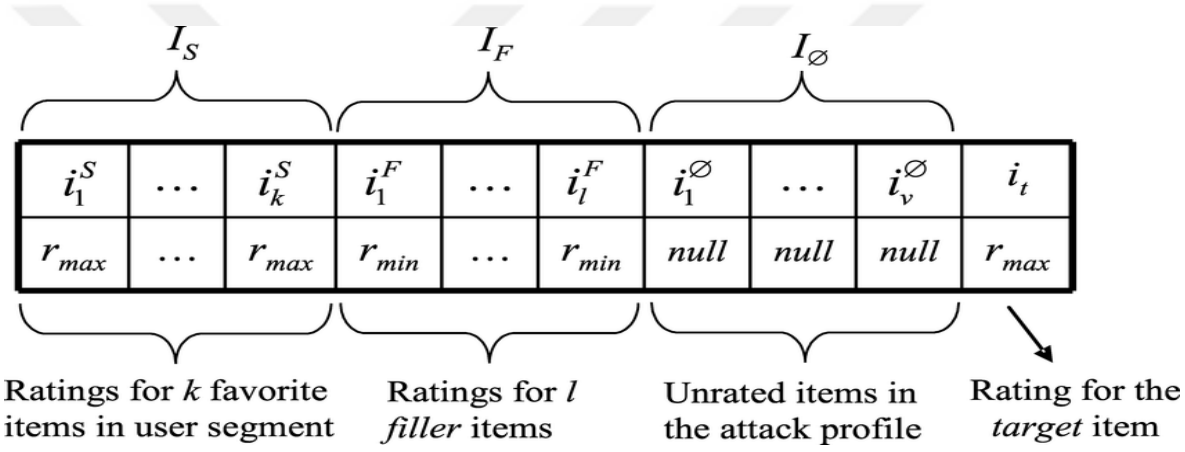
Bu bölümde, şilin atakların nasıl yapıldığı, çalışmada kullanılan atak çeşitlerinden segment atağın işleyişi, atak sonrası sistemin başarısının değişimi ve segment atağın belirli parametrelerle başarısı incelenmektedir.

5.1 Segment Atak Profili

Segment atak belirli kategorideki kullanıcıları hedefler, bu kullanıcıların geçmişte yöneldiği bir kategoride benzer sahte profiller oluşturularak hedef ürün, *a'* nın öneri

listesine sokulmaya çalışılır. Atak profili oluşturulurken kullanıcının geçmişte sıklıkla izlediği kategorideki filmlere yüksek oy verilirken, diğer filmlerin oyları düşük tutulur. Bu sayede kategorideki filmleri beğenmiş kullanıcılar ile atak kullanıcıları yüksek benzerlik gösterir ve önerilmesi istenilen ürünün kişinin öneri listesine girme ihtimali artar.

Segment atağı gerçekleştirecek sahte kullanıcıların oluşturulup sisteme dahil edilmesi oldukça kolaydır. Kategori bilgilerini öğrenmek için öneri sistemi ile ilgili ekstra bilgi sahibi olmaya gerek olmadan, sadece sisteme dahil olmak yeterlidir. Bu nedenle kötü niyetli kullanıcılar sahte segment atak profili oluştururken zorlanmadan sistemi kendi amaçlarına uygun manipüle edebilirler.



Şekil 5.1 *Segment atak genel profili*

Şekil 5.1 e göre genel bir segment atak profili gösterilmiştir Mobasher (2006). Segment içinden *seçilen ürünlere(selected items)* ve önerilmesi istenen *hedef ürüne(target item)* maksimum oy değeri olan 5 puan verilirken, bunların dışında kalan filmlerden rastgele oluşturulmuş belirli sayıda film seçilir. *Doldurulacak ürünler(Filler items)* denilen bu filmlerin sayısı algoritmada *Doldurma Büyüklüğü(Filler Size)* denilen değer tarafından belirlenir. Bu filmlere ise en düşük oyu temsil eden 1 değeri verilir. Böylelikle gerçek olmayan fakat hedef kategorideki kullanıcılarla yüksek benzerlik gösteren atak profili oluşturulmuş olur.

5.2 Deneyler ve Sonuçları

Tez içeriğinde MovieLens veri setinden, komedi ve drama kategorisinde film izlemiş kullanıcılara özgü çalışmalar yapılmıştır. 505 adet komedi filmi 725 adet drama filmi atak profili için segment verisini oluşturur.

Atak büyüklüğü(Attack size) sisteme kaç tane sahte profil ekleyeceğimizi söyleyen değerdir. Sistemde yer alan deneme kullanıcılarının sayısı üzerinden hesaplanır. Örneğin 700 adet deneme kullanıcısının olduğu bir sistemde, %5 lik bir atak büyüklüğü 700*5/100 adet atak profiline denk gelir. Yani atak büyüklüğü %5 olduğunda 35 adet profil saf deneme kullanıcısı verisine eklenir. Artık öneri sistemi, sistemde 735 adet kullanıcı varmış gibi çalışır ve bu kullanıcıların üzerinden öneri üretir.

Doldurma Büyüklüğü doldurulacak ürünlerin sayısını belirleyen değerdir. Seçilmiş ürünler haricindeki tüm oylanabilir ürünler üzerinden hesaplanır. Toplamda 1682 film içeren veriden 5 tane film seçildiğinde, 1677 film kalır ve bunların arasından doldurulacak ürünler seçilir. Örneğin %5 lik bir doldurma büyüklüğü, 1677*5/100 hesabına göre 83 adet film rastgele seçilerek 1 puan verileceği anlamına gelir.

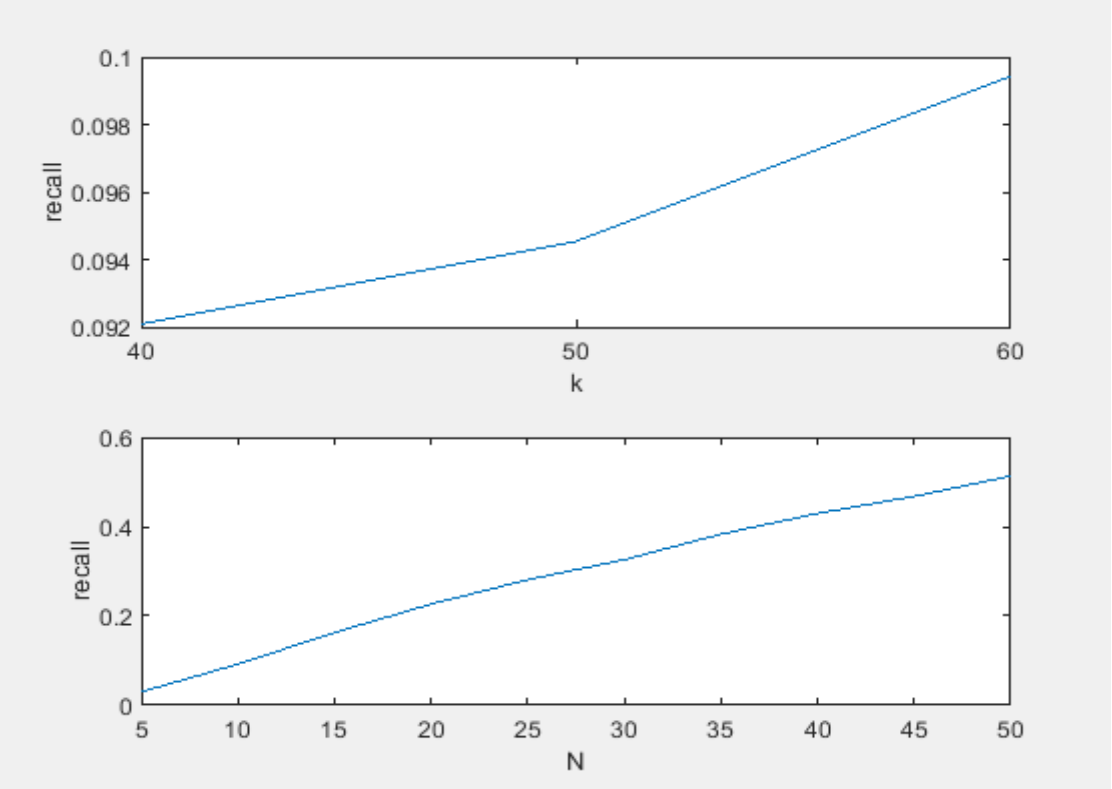
Belirli kategoriye ait filmlerin her biri için kaç kullanıcı tarafından 3 ten büyük oy aldıkları bilgisi tutulmuştur. Bu bilgiye göre, en fazla yüksek oy alan filmler en popüler filmler olarak düşünülmüştür. Filmler, popülerlik sırasına göre büyükten küçüğe doğru sıralanıp, en büyük ilk 5 film segment atak profillerinde seçilmiş filmler olarak belirlenmiştir. Burada amacımız, atak profillerinin gerçeğe yakın oluşturulması, dışardan bakıldığında sahte profillerin görülmesi ihtimalini azaltarak atağın etkisini güçlendirmektir. Aynı zamanda atak kullanıcılarının kategorideki popüler filmlerine oy verilmesi ile hedef kullanıcılarla benzerliği yakalamak amaçlanmaktadır.

4.3 kısmında anlatılan üst-N listesi oluşturulurken, her test kullanıcısı için tahmin üretilen ama kullanıcıya en uygun N tane film listesine giremeyen diğer filmlerin listesi ayrı bir yerde sıralı halde tutulur. Bu listede her bir kullanıcı için üst-N listesine girememiş kategoriye ait filmler yer alır. Bu listedeki filmler atak yaparken kullanılmak üzere tutulmuştur. Listede en çok yer alan filmler dışarıda kalmış olmasına rağmen birçok kullanıcının öneri listesine girebilme ihtimali yüksek filmlerdir. Bu özelliğe sahip listede en çok yer alan 5 adet film atak yapılacak hedef ürünler olarak belirlenmiştir.

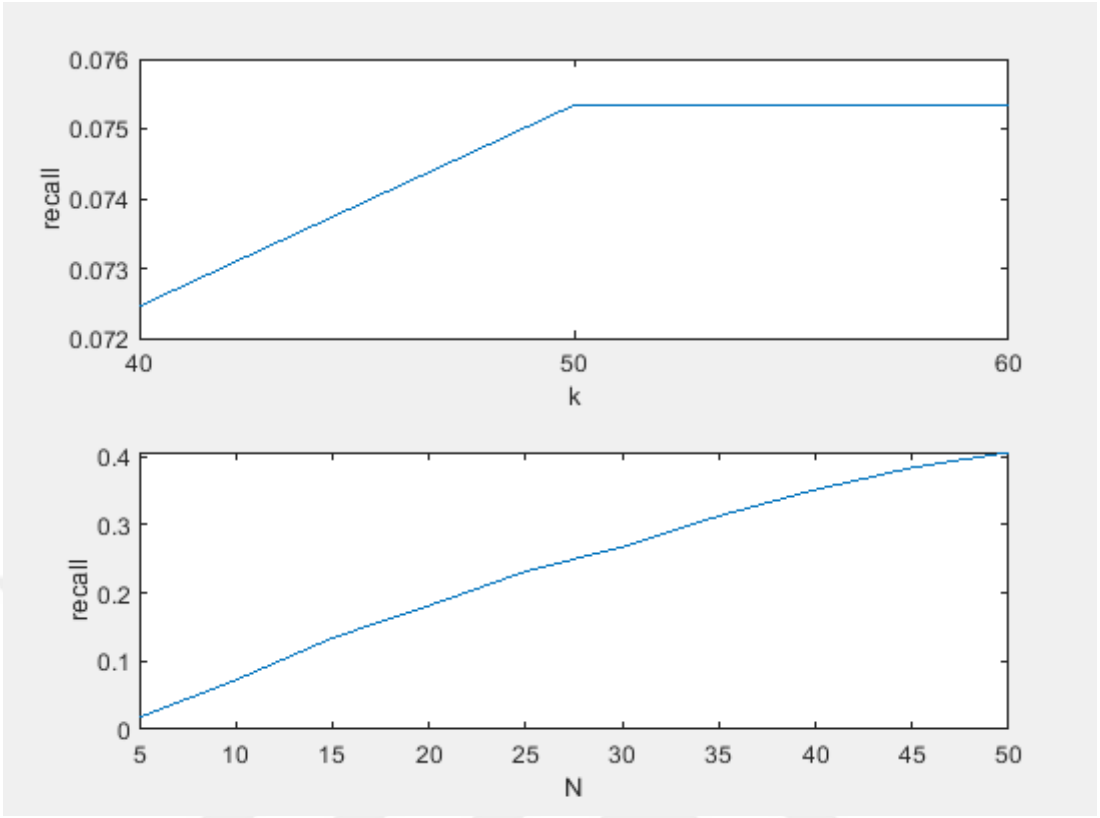
Bu kapsamda oluşturulan atak profilinde seçili ürünler kısmını tanımlayan, en popüler 5 adet filme en yüksek oy olan 5 puan verilmiştir. Hedef ürünler kısmını tanımlayan, atak listesinde en çok bulunan 5 filmin her biri, tüm atak profillerine bölünecek şekilde oy değeri 5 puan verilmiştir. Böylelikle bir atak profilinde bir hedef ürün olması sağlanmıştır. Doldurulacak ürünleri tanımlayan, doldurma büyüklüğüne göre rastgele seçilmiş filmlere en düşük oy olan 1 puan verilmiştir. Bunların dışında kalan filmlerin oy değerleri bulunmamaktadır, şekil 5.1deki oylanmamış filmlere karşılık gelir.

5.2.1 Atak sonrası sistemin başarısı

Deneyler için %14lük atak büyüklüğü ile 98 adet atak kullanıcısı oluşturulmuş olup, doldurma büyüklüğü %15 seçilmiştir. Sahte kullanıcılar deneme kullanıcılarına eklenerek üst-N listesinin başarı oranı tekrar ölçülmüştür. Deneyler iki kategori için ayrı ayrı yürütülmüştür. Segment atak sonrası duyarlılık değişimi iki kategori için grafiklerdeki gibidir.



Şekil 5.2 *Segment atak sonrası duyarlılık(recall) değişimi-MovieLens(komedi kategorisi)*

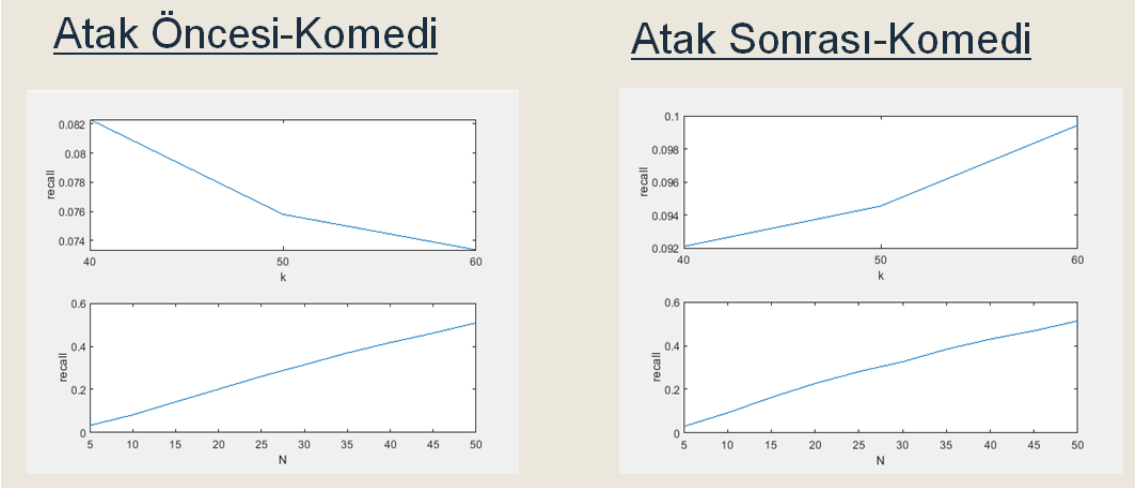


Şekil 5.3 S*egment atak sonrası duyarlılık(recall) değişimi-MovieLens(drama kategorisi)*

Grafikler incelendiğinde, atak sonrası yine iki kategorideki yönelimin aynı olduğu görülmektedir. Ancak komşuluk sayısının yönelimi atak öncesine göre değişmektedir. Atak öncesinde komşuluk sayısı arttıkça duyarlılık değeri azalarak devam ederken, atak sonrasında artış eğiliminde olduğu görülmektedir. N değerinin artması ile atak öncesi ve atak sonrası yönelimin aynı şekilde artarak devam ettiği görülmektedir.

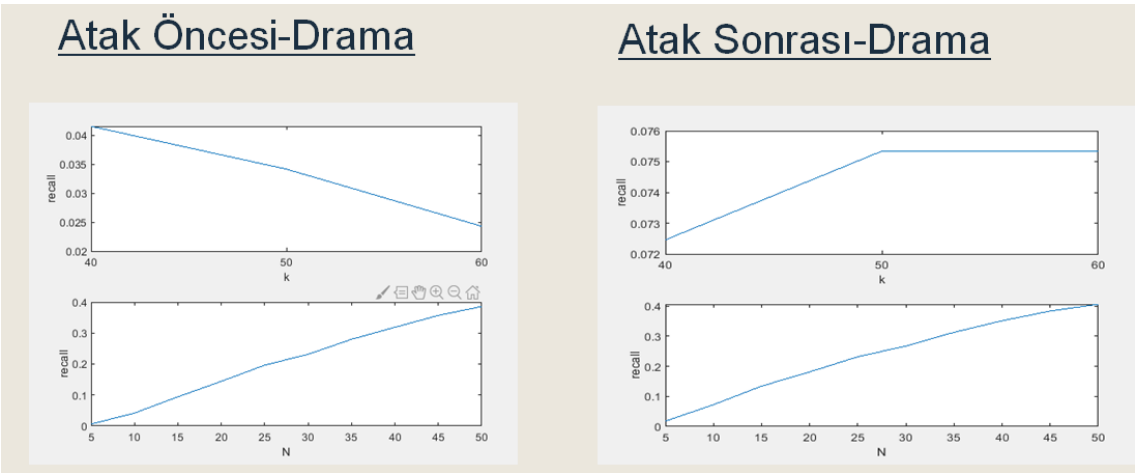
5.2.2 Atak öncesi ve sonrası durumun karşılaştırılması

Gerçekleştirdiğimiz deneylerde Movielens veri kümesinden komedi ve drama filmi kategorilerine segment atak yapılmıştır. Atak yapılmadan önceki ve sonraki grafiklerin kategori tabanında yan yana getirilerek değişimleri aşağıda incelenebilir.



Şekil 5.4 *Atak öncesi ve sonrası komedi kategorisinde duyarlılık(recall) değişimi*

Komedi filmleri kategorisine yapılan atağın, *k* parametresinin duyarlılığa etkisini zıt yönde değiştirdiği görülmektedir. Bu değişimin, atak kullanıcıları sisteme eklendikten sonra, *a*'ya daha yakın komşuların bulunarak yapılan önerilerin başarısının artmasından kaynaklandığı söylenebilir. N parametresinin artması ile duyarlılığın artışının atak sonrasında daha fazla olduğu görülmektedir. Bu artışın yine aynı sebepten sahte komşuların öneriye olumlu katkıda bulunmasından dolayı olduğu söylenebilir.



Şekil 5.5 *Atak öncesi ve sonrası drama kategorisinde duyarlılık(recall) değişimi*

Drama kategorisinde, atak sonrasında *k* parametresi atak öncesindeki başarıyı düşürücü etkisinden arttırıcı etkiye dönüştürmüştür. Duyarlılığın artışının komşu

seçimine katılan atak kullanıcılarının *a* ile benzerliğinden dolayı olduğu düşünülebilir. N sayısı arttığında atak sonrasında duyarlılık değişiminin daha olumlu olmasının, kaliteli komşuların öneri hesabına katılarak isabetli öneri sayısını arttırmasından dolayı olduğu çıkartılabilir.

İki kategori için grafikteki değişimler incelendiğinde, genel olarak atağın sistemin başarısını olumlu yönde etkilediği görülmektedir. Uygulanan segment atağın kategori bazında başarılı olduğu söylenilebilir. Sahte kullanıcıların öneri sistemine dahil olarak, kullanıcılara yapılan önerileri etkilediği ve sistemdeki kullanıcılarla benzerlik göstererek öneri hesaplarına katıldıkları görülmektedir.

5.2.3 Segment atak başarısı

Deneyler için %14 büyüklüğünde atak boyutu ile 98 adet atak kullanıcısı oluşturulmuş olup, doldurma büyüklüğü %15 seçilmiştir. Sahte kullanıcılar deneme kullanıcılarına eklenerek yeni deneme kullanıcısı kümesi üst-N listesi oluşturmak için öneri sistemine sokulmuştur. Yeni önerilen ürünler ile eskiden önerilen ürünlerin bilgisi saklanarak, hedef ürünlerden yüzde kaçının kullanıcıların listesine girebildiği hesaplanmıştır. 243 adet test kullanıcısından yüzde kaçının ataktan etkilendiği bilgisi de eklenmiştir. İlgili veriler aşağıdaki tabloda sunulmuştur.

Tablo 5.1 *Segment atağın kategori bazlı başarı bilgileri*

Kategori Bilgisi	Veri Sayısı	Test kullanıcılarının etkilenme yüzdesi	Hedef ürünlerin üst-N listesine girme yüzdesi
Drama Filmleri	725	%32,09	max=%100(52 kullanıcı) min=%20(4 kullanıcı)
Komedi Filmleri	505	%9,05	max=%100(13 kullanıcı) min=%20(2 kullanıcı)

Tablo incelendiğinde drama kategorisine gerçekleştirilen ataktan 243 kullanıcıdan %32,09 unun etkilendiği görülmektedir. 52 tane kullanıcının ataktan en çok etkilendiği ve her birinin öneri listesine hedef ürünlerin hepsinin girdiği görülmektedir. Ataktan en

az etkilenen 4 kullanıcının öneri listelerine ise hedef ürünlerden %20 sinin girdiği tablodan okunabilmektedir.

Komedi kategorisinde ise atak sonrasındaki durum incelendiğinde, 243 kullanıcının %9,05i ataktan etkilenirken, etkilenenlerden 13 tanesinin öneri listesine hedef ürünlerin tamamının girdiği, 2 kullanıcının ise en az etkilenerek hedef ürünlerin sadece %20sinin öneri listesine girebildiği tablodan okunabilmektedir.

Atak büyüklüğü ve doldurma büyüklüğüne göre eklenen sahte kullanıcıların özellikleri değiştiğinden dolayı, üst-N listesini etkileme oranı da değişiklik gösterir. Atak büyüklüğünün ve doldurma büyüklüğünün atak üzerindeki etkisi ve dolayısıyla test kullanıcılarının etkilenme yüzdelerini görebilmek için bazı deneyler yapılmıştır.

Tablo 5.2 de doldurma büyüklüğü %15 e sabitlenerek atak büyüklüğü parametrelerle değiştirilerek test kullanıcılarının her büyüklük için, yüzde kaçının ataktan etkilendiği test edilerek çıkan veriler not edilmiştir. Atak büyüklüğü %5, %10 ve %20 olduğunda yani oluşturulacak atak kullanıcılarının sayısı arttığında oluşan değişim gözlemlenmiştir.

Tablo 5.2 *Atak büyüklüğüne göre test kullanıcılarının etkilenme yüzdesi*

Atak Büyüklüğü	**%5**	**%10**	**%20**
Test kullanıcılarının etkilenme yüzdeleri	%8.64	%9.05	%9.46

Tablo 5.3 te ise atak büyüklüğü %15e sabitlenerek doldurma büyüklüğü parametreler değiştirilerek kullanıcıların etkilenme yüzdeleri tespit edilip veriler paylaşılmıştır. Doldurma büyüklüğünün, %5 en düşük büyüklük, %80 en yüksek büyüklük olacak şekilde atak üzerindeki etkisi incelenmiştir.

Tablo 5.3 *Doldurma büyüklüğüne göre test kullanıcılarının etkilenme yüzdesi*

Doldurma Büyüklüğü	**%5**	**%10**	**%20**	**%40**	**%60**	**%80**
Test kullanıcılarının etkilenme yüzdeleri	%2.46	%5.34	%9.87	%16.04	%20.57	%23.45

Tablolar incelendiğinde; atak büyüklüğü ve doldurma büyüklüğünün artması ile sistemdeki kullanıcıların etkilenme yüzdesinin arttığı görülmektedir. İki büyüklüğün her birinin artması atağın etkisini arttırdığı için, atağın daha başarılı olduğu söylenilebilir. Atak büyüklüğü ve doldurma büyüklüğü arttığında, bazı test kullanıcılarıyla benzeşme oranı artabilir, bu durum hedef ürünün hedef kullanıcının listesine girmesini sağlayabilir.

Atak büyüklüğü arttıkça sisteme eklenecek sahte profillerin sayısı artar. Bu durumda test kullanıcılarının atak kullanıcılarından en az biriyle, benzer komşu olma olasılığı yükselir. Bu durum hedef ürünlerin test kullanıcısının listesine girmesine neden olarak başarıyı arttırır.

Bir atak profilinin doldurma büyüklüğünün artmasıyla, gerçek kullanıcılara daha yakın sahte kullanıcılar elde edilir. Dolayısıyla test kullanıcılarıyla atak kullanıcılarının benzeşme ihtimali artarak, hedef ürünlerin kullanıcıların listesine girme olasılığı artar.

6. SONUÇLAR

Tez çalışmasında öneri sistemlerinin en popüler uygulamalarından biri olan üst-N listesinin belirli bir kategori üzerinde çalışması incelenmiştir. Gerçek veri setinde kullanıcı film değerlendirmeleri üzerinde belirli bir film kategorisinde yapılan segment atağın sisteme etkisinin incelenmesi, literatür açısından bir yenilik olmuştur.

Üst-N listesi oluşturan öneri algoritmasının komşuluk ve listeye alınacak öneri ürünlerinin sayısı parametrelerine göre değişimleri iki farklı kategori için de benzer olduğu sonucuna ulaşılmıştır. Öneri üretirken kullanılacak en benzer komşu seçim sayısı arttıkça, başarının azalması seçilen komşuların kalitesinin düşmesi ile bağlantılı olduğu söylenilebilir. Fazla komşu kullanılarak üretilecek öneriler daha doğru olabildiği gibi bu durumdakine benzer daha başarısız da olabilir. Bu seçilen komşu kullanıcının öneri için ne kadar kaliteli bilgi verebileceği ile ilgilidir. Öneri listelerine dahil edilecek ürün sayısının artmasının başarılı önerileri doğurması, daha fazla ürünün listeye alınması ile hedef ürünün listeye girmesini kolaylaştırmasından dolayıdır. İsabet oranı arttığı için sistemin başarısının da yükseldiği gözlemlenmektedir.

Kategori alanındaki film sayısı arttığında başarının düşmesi, ürün sayısının artmasının bilginin kalitesiyle doğru orantılı olmayabileceğini göstermektedir. Drama filmleri daha fazla sayıda olmasına rağmen komedi filmlerine göre daha az ve kalitesiz bilgi içeriyor olabileceği deney sonuçlarına bakarak söylenebilir.

Kullanıcı ürün değerlendirmelerinin epey büyük olduğu veri kümesi üzerinde çalıştırılan üst-N öneri sistemlerinin başarısının, daha küçük kümeye sahip veri setine oranla düşük olduğu görülmektedir. Buna fazla sayıda kullanıcı ve kalabalık verinin neden olduğu söylenebilir. Seçilen komşu sayısının artması bir limite kadar öneriye olumlu yönde etki ederken, daha fazla komşunun katkısı olumsuz yönde etki edebilir. Algoritmaya dahil olan komşu deneme kullanıcılarının belirli sayıya kadar a ile benzerliği öneriye olumlu katkı yaptığı, komşu sayısının daha çok artması ile yararlı kullanıcı yerine a ile az benzeşen komşuların dahil edilmesinden dolayı önerinin kalitesizleştiği düşünülebilir.

Üst-N listesi üreten öneri sistemlerine segment atak yapılarak oluşturulan deney sonuçlarına göre sistemin gürbüzlüğü incelenmiştir. Farklı kategoriler üzerine gerçekleştirilen segment ataklarının grafikler incelendiğinde sistemin başarısını arttırıcı

yönde etkisi olduğu söylenebilir. Buna neden olarak deneme kullanıcılarının atak kullanıcılarıyla birleşince sayısının artmasından dolayı, komşuluk seçiminde daha yakın komşular bulunarak isabet sayısının artması gösterilebilir. Atak kullanıcıları sisteme dahil edildiğinde, deneme kullanıcılarında o segment bazında benzer kullanıcılar çoğalacağı için yapılan önerilerin isabet oranının artmış olabileceği söylenilebilir.

Segment atağın başarısı incelendiğinde, atakların daha büyük bir veri kümesinde daha çok etki ettiğini görebiliriz. Deney sonuçlarına göre yüzdelere bakıldığında hedef ürünü kullanıcının listesine itmede başarılı olduğu söylenilebilir. Her hedef ürünü öneri listesine alamasa da test kullanıcılarının etkilenme yüzdesinin artması, liste dışında kalan elemanlardan daha çok hedef ürün seçilmesi yoluyla sağlanabilir. Üst-N listesinin dışında kalan elemanlarından en çok bulunan ürünü hedef seçme fikrinin doğru bir yol olduğu düşünülebilir.

Atak büyüklüğü ile doldurma büyüklüğü parametrelerinin segment atağın başarısında önemli bir rol oynadığı sonuçlara bakarak yorumlanabilir. Atak kullanıcılarının sayısının artmasının ve doldurma büyüklüğü ile daha benzer atak kullanıcılarının oluşturulmasının genel olarak atağın başarısını olumlu yönde etkilediği söylenebilir.

Gelecek çalışmalarda, bu tez çalışmasında kullanılan kategorilerden farklı kategoriler ve farklı veri setleri üzerinde çalışılabilir. Üst-N algoritmalarında çeşitli komşuluk ve öneri üretme algoritmaları geliştirilerek daha gürbüz üst-N öneri sistemleri için çalışılabilir. Segment atak oluştururken hedef ürün ve seçilmiş ürünlerin belirlenmesinde farklı metodlar uygulanıp sonuçlar incelenebilir. Üst-N listeleri için segment atak dışında diğer atak tiplerinin de sistemi nasıl etkileyeceği incelenebilir.

KAYNAKÇA

A.M. Turk, A. Bilge (2019). Robustness analysis of multi-criteria collaborative filtering algorithms against shilling attacks. Expert Systems with Applications, 115 (2019), pp. 386-402

Aggarwal, C., Wolf, J., Wu, K., ve Yu, P. 1999. Horting hatches an egg: A new graph-theoretic approach to collaborative filtering. In Proceedings of ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, ACM, New York.

Aggarwal, C.C. (2016a). Attack-resistant recommender systems, Recommender Systems. Springer, pp. 385–410.

Alper Bilge, Zeynep Batmaz ve Hüseyin Polat (2016). Maskelenmiş Veriler için Kümeleme-Tabanlı Şilin Atak Tespit Yöntemi

Athanasios N. Nikolakopoulos, Dimitris Berberidis, George Karypis and Georgios B. Giannakis. 2019. Personalized Diffusions for Top-N Recommendation. In Thirteenth ACM Conference on Recommender Systems (RecSys '19), September 16–20, 2019, Copenhagen, Denmark. ACM, New York, NY, USA, 9 pages.

Burke, R., Mobasher, B., ve Bhaumik, R. (2005a). Limited knowledge shilling attacks in collaborative filtering systems, Proceedings of 3rd International Workshop on Intelligent Techniques for Web Personalization (ITWP'05), held at 19th International Joint Conference on Artificial Intelligence (IJCAI'05), Edinburgh, Scotland. pp. 17–24.

Burke, R., Mobasher, B., Williams, C., ve Bhaumik, R. (2006a). Classification features for attack detection in collaborative recommender systems, Proceedings of the 12th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD'06), Philadelphia, PA, USA. pp. 542–547.

Burke, R., Mobasher, B., Williams, C., ve Bhaumik, R. (2006b). Detecting profile injection attacks in collaborative recommender systems, Proceedings of the 8th IEEE International Conference on E-Commerce Technology and the 3rd IEEE

International Conference on Enterprise Computing, E-Commerce, and E-Services (CEC/EEE'06), San Francisco, California. pp. 23–23.

Burke, R., O'Mahony, M.P., ve Hurley, N.J. (2015). Robust collaborative recommendation, Recommender Systems Handbook. Springer, pp. 961–995.

B. Sarwar, G. Karypis, J. Konstan, and J. Riedl. Item-based collaborative filtering recommendation algorithms. In WWW'01: 10th International World Wide Web Conference, 2001.

B. Yılmazel Developing techniques for robustness of privacy-preserving distributed collaborative filtering, 2016

B. Kanagal, A. Ahmed, S. Pandey, V. Josifovski, J. Yuan, ve L. GarciaPueyo, "Supercharging recommender systems using taxonomies for learning user purchase behavior," VLDB, 2012.

Bilsus, D. ve Pazzani, M. J. 1998. Learning collaborative information filters. In Proceedings of ICML. 46–53.

Breese, J.,Heckerman, D., ve Kadie, C. 1998. Empirical analysis of predictive algorithms for collaborative filtering. In Proceedings of the 14th Conference on Uncertainty in Artificial Intelligence. 43–52.

Chirita, P.A., Nejdl, W., ve Zamfir, C. (2005). Preventing shilling attacks in online recommender systems, Proceedings of the 7th Annual ACM International Workshop on Web Information and Data Management (WIDM'05), Bremen, Germany. pp. 67–74.

Evangelia Christakopoulou and George Karypis. 2018. Local Latent Space Models for Top-N Recommendation. In KDD '18: The 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, August 19–23, 2018, London, United Kingdom. ACM, New York, NY, USA, 9 pages

G. Karypis. Evaluation of item-based top-n recommendation algorithms. In CIKM '01: Proceedings of the tenth international conference on Information and knowledge management, pages 247–254, New York, NY, USA, 2001.

Güneş, I., Bilge, A., ve Polat, H. (2013b). Shilling attacks against memory-based privacy-preserving recommendation algorithms. KSII Transactions on Internet and Information Systems (TIIS) 7(5), 1272–1290.

Güneş, I., Kaleli, C., Bilge, A., ve Polat, H. (2014). Shilling attacks against recommender systems: A comprehensive survey. Artificial Intelligence Review 42(4), 767–799.

H.-N. Kim, A.-T. Ji, H.-J. Kim, and G.-S. Jo. Error-based collaborative filtering algorithm for top-n recommendation. In The Joint International Conferences on Asia-Pacific Web Conference and Web-Age Information Management (APWeb/WAIM), pages 594–605, Huang Shan, China, June 2007.

Herlocker, J., Konstan, J., Borchers, A., ve Riedl, J. 1999. An algorithm framework for performing collaborative filtering. In Proceedings of SIGIR. ACM, New York, 77–87.

J. Herlocker, J. A. Konstan, ve J. Riedl, "An empirical analysis of design choices in neighborhood-based collaborative filtering algorithms," Information retrieval, vol. 5, no. 4, 2002

J. Lee, M. Sun, ve G. Lebanon, "A comparative study of collaborative filtering algorithms," arXiv preprint arXiv:1205.3193, 2012.

Kaleli, C., ve Polat, H. (2013). Robustness analysis of Na¨ıve Bayesian classifier-based collaborative filtering, E-Commerce and Web Technologies. Springer, pp. 202–209.

Konstan, J., Miller, B., Maltz, D., Herlocker, J., Gordon, L., ve Riedl, J. 1997. GroupLens: Applying collaborative filtering to Usenet news. Commun. ACM 40, 3, 77–87.

Kitts, B., Freed, D., ve Vrieze, M. 2000. Cross-sell: A fast promotion-tunable customer–item recommendation method based on conditional independent probabilities. In Proceedings of ACM SIGKDD International Conference. , ACM, New York, 437–446.

Long, Q., ve Hu, Q. (2010). Robust evaluation of binary collaborative recommendation under profile injection attack, Proceedings of the 2010 IEEE International Conference on Progress in Informatics and Computing (PIC'10), Shanghai, China. pp. 1246–1250.

M. R. McLaughlin and J. L. Herlocker. A collaborative filtering algorithm and evaluation metric that accurately model the user experience. In SIGIR '04: Proceedings of the 27th international ACM SIGIR conference on Information Retrieval, pages 329–336, New York, NY, USA, 2004

M. Deshpande and G. Karypis. Item based top-n recommendation algorithms. ACM Transactions on Information Systems, 22:143–177, 2004.

Mehta, B., ve Hofmann, T. (2008). A survey of attack-resistant collaborative filtering algorithms. IEEE Data Engineering Bulletin 31(2), 14–22.

Mobasher, B., Burke, R., Bhaumik, R., ve Williams, C. (2005). Effective attack models for shilling item-based collaborative filtering systems, Proceedings of the 2005 WebKDD Workshop, held in conjuction with ACM SIGKDD'05, Chicago, IL, USA. pp. 13–23.

Mobasher, B., Burke, R., Williams, C., ve Bhaumik, R. (2006b). Analysis and detection of Segment-focused attacks against collaborative recommendation, Proceedings of the 7th International Conference on Knowledge Discovery on the Web: Advances in Web Mining and Web Usage Analysis (WebKDD'05), Chicago, IL, USA. pp. 96–118.

Mobasher, B., Burke, R., Bhaumik, R., ve Sandvig, J.J. (2007a). Attacks and remedies in collaborative recommendation. EEE Intelligent Systems 22(3), 56– 63.

O'Mahony, M.P., Hurley, N.J., ve Silvestre, G.C. (2002). Promoting recommendations: An attack on collaborative filtering, Proceedings of the 13th International Conference on Database and Expert Systems Applications (DEXA'02), Aix-en-Provence, France. pp. 494–503.

O'Mahony, M.P. (2004). Towards Robust and Efficient Automated Collaborative Filtering. PhD dissertation. University College Dublin. Department of Computer Science, Belfield, Dublin 4, Ireland.

O'Mahony, M.P., Hurley, N.J., ve Silvestre, G. (2004b). Utility-based neighbourhood formation for efficient and robust collaborative filtering, Proceedings of the 5th ACM Conference on Electronic Commerce (EC'04), New York, NY, USA. pp. 260–261.

O'Mahony, M.P., Hurley, N.J., ve Silvestre, G.C. (2004c). Efficient and secure collaborative filtering through intelligent neighbour selection, Proceedings of the 16th European Conference on Artificial Intelligence (ECAI'04), Valencia, Spain. pp. 383–387.

O'Mahony, M.P., Hurley, N.J., ve Silvestre, G.C. (2005). Recommender systems: Attack types and strategies, Proceedings of the 20th National Conference on Artificial Intelligence (AAAI'05), Pittsburgh, Pennsylvania. pp. 334–339.

P. Cremonesi, Y. Koren, ve R. Turrin, "Performance of recommender algorithms on top-n recommendation tasks," in RecSys, 2010

Resnick, P., Iacovou, N., Suchak, M., Bergstrom, P., ve Riedl, J. 1994. GroupLens: An open architecture for collaborative filtering of netnews. In Proceedings of CSCW.

Resnick, P., ve Sami, R. (2007). The influence limiter: Provably manipulationresistant recommender systems, Proceedings of the 2007 ACM Conference on Recommender Systems (RecSys'07), Minneapolis, MN, USA. pp. 25–32.

Shardanand, U. ve Maes, P. 1995. Social information filtering: Algorithms for automating "word of mouth". In Proceedings of the ACM CHI'95 Conference on Human Factors in Computing Systems. ACM, New York, 210–217.

Sarwar, B., Karypis, G., Konstan, J., ve Riedl, J. 2000. Analysis of recommendation algorithms for e-commerce. In Proceedings of ACM E-Commerce. ACM, New York.

Su, X.F., Zeng, H.J., ve Chen, Z. (2005). Finding group shilling in recommendation system, Proceedings of the Special Interest Tracks and Posters of the 14th International Conference on World Wide Web (WWW'05), Chiba, Japan. pp. 960–961.

T.Srikanth, M.Shashi, "New Metrics for Effective Detection of Shilling Attacks in Recommender Systems", International Journal of Information Engineering and Electronic Business(IJIEEB), Vol.11, No.4, pp. 33-42, 2019. DOI: 10.5815/ijieeb.2019.04.04

Van Roy, B., ve Yan, X. (2009). Manipulation-resistant collaborative filtering systems, Proceedings of the 3rd ACM Conference on Recommender Systems (Rec- Sys'09), New York, NY, USA. pp. 165–172.

Van Roy, B., ve Yan, X. (2010). Manipulation robustness of collaborative filtering. Management Science 56(11), 1911–1929.

Zhou W, Wen J, Qu Q, Zeng J, Cheng T (2018) Shilling attack detection for recommender systems based on credibility of group users and rating time series. PLoS ONE 13(5): e0196533.