Journal of the Faculty of Engineering and Architecture of Gazi University 36:4 (2021) 1909-1921

Mühendislik Mimarlık Fakültesi Dergisi
Journal of The Faculty of Engineering and Architecture of Gazi University

Elektronik / Online ISSN : 1304 - 4915
Basılı / Printed ISSN : 1300 - 1884

Bi-level multiple attack type protection models for defense planning of critical systems

Orkun Başkan[1]*, Müjgan Sağır[2]

[1]Department of Industrial Engineering, Faculty of Engineering, Eskisehir Technical University, Eskisehir, 26555, Turkey
[2]Department of Industrial Engineering, Faculty of Engineering and Architecture, Eskisehir Osmangazi University, Eskisehir, 26480, Turkey

Highlights:

- Bi-level interdiction / protection models are discussed.
- A new bi-level R_eIMF protection model which considered defense and attack types.
- A new bi-level SD − R_eIMF protection model, which is capacity constraint and primarily maintain supply-demand balance.

Keywords:

- Interdiction problem
- Protection problem
- Bi-Level programing
- Defense planning
- Attack types
- Supply-Demand Balance

Article Info:

Research Article
Received: 04.09.2019
Accepted: 21.03.2021

DOI:

10.17341/gazimmfd.615372

Correspondence:

Author: Orkun Başkan
e-mail: orkunbaskan@eskisehir.edu.tr
phone: +90 532 786 3093

Graphical/Tabular Abstract

This paper presents two new mathematical models for defense planning of critical systems. The decision of which facilities under the risk of different attacks are to be protected to meet the demand of a particular zone is of interest. In previous studies, different attack and defence types have been disregarded for this problem. Our models consider different attack and defense options. First model proposed is called as R_eIMF which considers these different attack and defense types, second model is called as SD − R_eIMF and this model tries to disrupt the supply-demand balance. These models correspond to upper and lower level models. We assume that upper level represents the defender model and the protection strategy is the output of this model, and lower level represents the attacker model, and attacker decides where to attack by having the information of which facilities are protected.

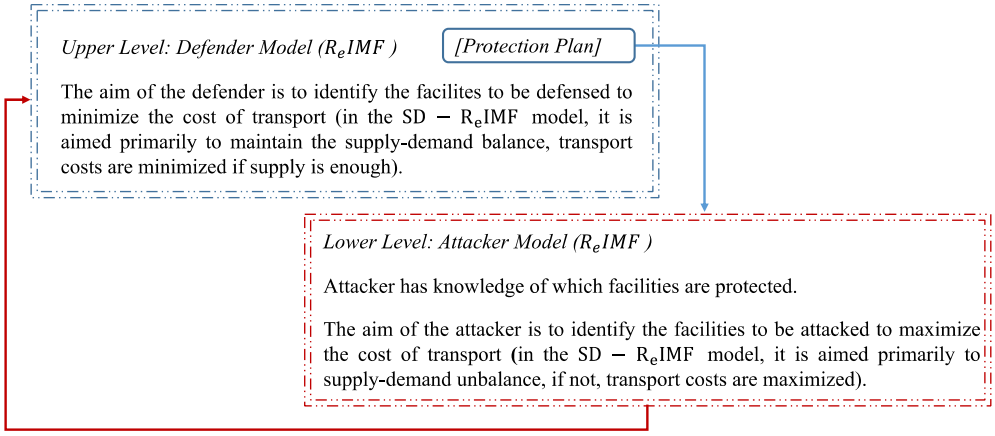


Figure A: Bi-level New R_eIMF and SD − R_eIMF Protection Models

Purpose: The aim of this study is to consider different attack and defense types in defense planning of critical regions. In addition, it is aimed to determine the best defense planning against attacks to disrup the supply-demand balance when resources are limited.

Theory and Methods: Based on Scappara (2008)'s RIMF model, two new mathematical models have been proposed to solve the protection problems. These models are bi-level models. Upper level is defense's level and lower level is attacker's level.

Results: The models find effective solutions for problems including attack and defense types while providing supply and demand balance for capacity limited problems. We think that proposed models are better representations of the real cases.

Conclusion: The proposed R_eIMF and SD − R_eIMF models found the optimum solution. The models are able to produce protection plans and facility – demand point matching. Due to the security reasons, it is not convenient to apply the proposed models for governmental level problems or for military applications without permissions and not possible even to reach the real case data but we are ready to submit our findings, besides the models can be used also for some other kind systems such as electrical systems that are also subject to technical risks that are also threats to interrupt the service availability.

Journal of the Faculty of Engineering and Architecture of Gazi University 36:4 (2021) 1909-1921

Mühendislik Mimarlık Fakültesi Dergisi
Journal of The Faculty of Engineering and Architecture of Gazi University

Elektronik / Online ISSN : 1304 - 4915
Basılı / Printed ISSN : 1300 - 1884

Kritik sistemlerin savunma planlaması için iki seviyeli çoklu saldırı tipli koruma modelleri

Orkun Başkan[1]*, Müjgan Sağır[2]

[1]Eskişehir Teknik Üniversitesi, Mühendislik Fakültesi, Endüstri Mühendisliği Bölümü, 26555, Eskişehir, Türkiye
[2]Eskişehir Osmangazi Üniversitesi, Mühendislik Mimarlık Fakültesi, Endüstri Mühendisliği Bölümü, 26480, Eskişehir, Türkiye

Ö N E Ç I K A N L A R

- İki seviyeli Yasaklama/ Koruma Modelleri ele alınmıştır.
- Savunma ve Saldırı Tiplerinin göz önüne alındığı yeni iki Seviyeli R_eIMF koruma Modeli
- Kapasite Kısıtlı, Arz-Talep dengesi sağlama öncelikli, yeni İki seviyeli SD − R_eIMF koruma Modeli

Makale Bilgileri
Araştırma Makalesi
Geliş: 04.09.2019
Kabul: 21.03.2021

DOI:
10.17341/gazimmfd.615372

Anahtar Kelimeler:
Yasaklama problemleri, koruma problemleri, iki seviyeli programlama, savunma planlaması, saldırı tipleri, arz-talep dengesi

ÖZ

Kritik tesisler, bir ülke için yüksek önem düzeyine sahip, herhangi bir sebeple savaş, terörist saldırı, doğal afetler vb. gibi kendilerine verilecek zarar neticesinde, ülkeyi önemli ölçüde etkileyebilecek tesislerdir. Bu tesislerin korunması önemli problemlerdendir. Bu çalışma bir kritik bölgenin talebinin kesintisiz olarak sağlanması için hangi tesislerin korunacağının belirlenmesine yönelik tesis koruma problemlerindendir. Önceki çalışmalarda göz ardı edilmiş olan farklı saldırı tipleri ve karşı gelen savunma tipleri göz önüne alınmış, ayrıca sınırlı kaynaklara sahip kritik sistemler için arz talep dengesinin bozulmasına yönelik öncelikli amaç modele dahil edilmiştir. Bu çalışma kritik tesislerin savunma problemi için iki yeni matematiksel model önermektedir. Modellerin katkısı sırası ile farklı saldırı - savunma tiplerini ve arz-talep dengesini dikkate almaktır. İlk model saldırı ve koruma tiplerini göz önüne alan iki seviyeli R_eIMF ve arz talep dengesini bozma amaçlı saldırıların göz önüne alındığı SD − R_eIMF'dir. İki modelde literatürde yer alan RIMF (r-interdiction median problem with fortification) modelini temel almaktadır. Modeller gerçek verilere ulaşmanın zorluğu nedeni ile türetilen örnek problem setleri kullanılarak test edilmiş ve deneysel sonuçlarla yöntemin kullanılabilirliği ortaya konmuştur. R_eIMF modeli sınırsız kapasiteli problemler için SD − R_eIMF modeli ise sınırlı kapasiteli problemlere çözüm sunmaktadır.

Bi-level multiple attack type protection models for defense planning of critical systems

H I G H L I G H T S

- Bi-level interdiction / protection models are discussed.
- A new bi-level R_eIMF protection model which considered defense and attack types.
- A new bi-level SD − R_eIMF protection model, which is capacity constraint and primarily maintain supply-demand balance

Article Info
Research Article
Received: 04.09.2019
Accepted: 21.03.2021

DOI:
10.17341/gazimmfd.615372

Keywords:
Interdiction problem, protection problem, bi-level programing, defense planning, attack types, supply-demand balance

ABSTRACT

Critical infrastructures are so vital for a country that their destruction or incapacity with war, terrorist attack and natural disasters may have irrecoverable effects on security systems together with other social, economic, and public systems. The protection of these facilities is one of the important problems. This study is one of the facility protection problems to determine which facilities will be protected to ensure the uninterrupted demand of a critical zone. Different attack types and counter defense types, which were ignored in previous studies, were taken into account in this study. Disrupting the supply-demand balance for critical systems with limited resources is also included in the model. This paper presents two new mathematical models for the defense of critical infrastructure systems. The contribution of our models is considering different types of attacks and defense options and disrupting the supply-demand balance. The first model is R_eIMF and considers different attack and defense types. The second model is SD − R_eIMF and considers supply-balance disruption. Both models are based on RIMF (r-interdiction median problem with fortification) model in the literature. Due to security reasons, it is not possible to find real data to apply the methodology to a real system in our case, therefore we developed a toy problem to solve the models proposed and discussed the results. R_eIMF model offers solution for problems with unlimited capacity and model SD − R_eIMF offers a solution to problems with limited capacity.

*Sorumlu Yazar/Yazarlar / Corresponding Author/Authors : *orkunbaskan@eskisehir.edu.tr, msagir@ogu.edu.tr / Tel: +90 532 786 3093

1. GİRİŞ (INTRODUCTION)

Kritik tesisler, bir ülke için yüksek önem düzeyine sahip, savaş, terörist saldırı, doğal afetler vb. gibi bir sebeple kendilerine verilecek zarar neticesinde ülkeyi önemli ölçüde etkileyebilecek tesislerdir. Bu tesislerde oluşabilecek zafiyet, güvenlik açığının oluşmasına, toplumsal yaşamın etkilenmesine ve ekonomik zararların oluşmasına yol açacaktır.

Ülkemizin bulunduğu coğrafya ve günümüz çıkar çatışmaları göz önüne alındığında çok çeşitli tehditler söz konusudur ve bu tehditlere karşı kritik tesislerin savunulması önemli konuların başında gelmektedir. NATO Genel Sekreteri Anders Fogh Rasmussen (2009-2014, NATO 12. Genel Sekreteri) günümüzdeki tehditleri 'küresel terörizm', 'balistik füzelerin yayılması' ve 'siber-güvenlik' olarak sınıflandırmıştır.

ABD Başkanlık politika direktifinde (PPD-21) 16 kritik sektör Tablo 1'de görüldüğü gibi belirlenmiştir.

Tablo 1. Kritik Sektörler (ABD Başkanlık Politika Direktifleri PPD-21)
(Critical Infrastructure Sectors (USA Presidential Policy Directive 21 PPD-21))

Kritik Sektörler	
Kimya Sektörü	Ticari tesisler
İletişim Sektörü	Kritik imalat sektörü
Barajlar	Savunma Sanayi Temelli sektörler
Acil Servisler	Enerji Sektörü
Finans Hizmetleri	Gıda ve Tarım Sektörü
Hükümet Tesisleri	Sağlık hizmetleri ve kamu Sağlığı
Bilgi Teknolojileri	Nükleer Reaktörler, maddeler ve atıklar
Ulaşım sistemleri	Su ve Atık su sistemleri

Ele aldığımız problemde kritik sistemleri tahrip etmek isteyen bir saldırgan ve kritik sistemleri koruma kararını veren bir savunan söz konusudur. Problem saldırgan-savunan ya da savunan-saldırgan şeklinde ele alınabilecek Stackelberg'in oyun teorisine dayanmaktadır [1]. Problem saldırgan açısından ele alınarak saldırganın amacının eniyilendiği modeller yasaklama (interdiction) modelleri, savunan açısından ele alınarak savunanın amacının eniyilendiği modeller ise koruma (fortification, protection) modelleri olarak adlandırılmaktadır.

Yasaklama/koruma modelleri yasaklanacak/korunacak kritik yapının, tesis ya da tesisler arasındaki bağlantılar olmasına göre literatürde tesis yasaklama/koruma modelleri ya da ağ yasaklama/koruma modelleri olarak çalışılmaktadır. Bu çalışmada problem, savunanın hangi tesisleri koruyacağı kararının verilmesi yönünde olup tesis koruma modeli ile ilgilidir. Temel olarak, ele alınan kritik alt yapı ve hizmetler değişmekle birlikte tüm problemler, saldırganın kritik sisteme en fazla zararı vermek, savunma planlamacısının ise koruma planını, oluşabilecek zararı enküçüklemek yönünde hareket ettiği bir yapıya dayanmaktadır.

Çalışmada, genel bir yasaklama/koruma problemi için saldırı tiplerindeki değişim göz önüne alınarak geliştirilen iki yeni matematiksel model sunulmuştur. Bu kapsamda belirli bir bölgeye kesintisiz olarak hizmet sağlamak amaçlanmaktadır. Burada hizmet sunan tesisler kritik tesisler, bu birimlerin hizmet sunduğu müşteriler ise talep noktaları olarak kabul edilmiştir ve bunlardan hangilerinin korunmasının en iyi karar olacağı araştırılmıştır. Bu çalışmada, Scaparra ve Church [2]'da sunulan iki seviyeli RIMF modeli temel alınarak gerçek durumu daha iyi ortaya koymayı hedefleyen iki yeni model önerilmiştir. İlk modelde saldırganın yasaklama çeşidinin ve yasaklama çeşidine göre koruma çeşitlerinin de birden fazla tipte olacağı "İki Seviyeli Çoklu Saldırı Tipli Koruma Modeli" olarak R_eIMF matematiksel modeli, ile hizmet sunan tesislerin kapasitelerinin kısıtlı olacağı ve saldırganın arz ve talep arasındaki dengeyi bozmayı hedefleyeceği göz önüne alınarak "Arz Talep Dengesi Bozma Amaçlı İki seviyeli Çoklu Saldırı Tipli Koruma Modeli" ($SD-R_e$IMF) sunulmuştur. Her iki durumun da ele alındığına önceki çalışmalarda rastlanmamıştır. Modellerin çözümü küçük bir örnek veri seti ile denenmiş ve sonuçları 4. bölümde paylaşılmıştır. Bu çerçevede ikinci bölümde konu ile ilgili literatür araştırması, üçüncü bölümde önerilen matematiksel modeller verilmektedir. Dördüncü bölümde yeni modeller örnek bir veri seti ile çözülmekte, son bölümde ise sonuçlara yer verilmektedir. Özetle çalışmanın literatüre katkısı şu şekilde özetlenebilir:

- Çalışmada, erişilebilen literatürde yer almayan aşağıdaki iki yeni model önerilmiştir.
  - Yeni model 1: İki Seviyeli Çoklu Saldırı Tipli Koruma Modeli (R_eIMF)
  - Yeni model 2: Arz Talep Dengesi Bozma Amaçlı İki seviyeli Çoklu Saldırı Tipli Koruma Modeli ($SD-R_e$IMF)
- Literatürde saldırı ve savuma tiplerinin tek tip olduğu varsayılmıştır. Gerçek hayatta ise saldırı tipleri ve karşılığında öne sürülebilecek savunma tipleri çeşitli olabilmektedir. Önerilen modellerde savunma ve saldırı tiplerinin çeşitli olabileceği durum göz önüne alınmıştır.
- Bir saldırganın saldırıdaki amacının her zaman maliyet değil, arz-talep dengesi bozma yönünde de olabileceği durum göz önüne alınmıştır ve buna dönük Yeni Model 2 geliştirilmiştir.
- Literatürde yapılan çalışmalarda genellikle hizmet sunan tesislerin kapasitelerinin sınırsız olduğu varsayılmaktadır. Oysa bu gerçekçi bir varsayım değildir. Yeni Model 2'de tesislerin kapasite sınırı göz önünde bulundurulmuş, bunun sonucu olarak da tedarikin karşılanamadığı durum modele dahil edilmiştir.
- Yeni Model 1 ve 2, literatürdeki RIMF modelini temel almaktadır. RIMF modeli, bir tesis hizmet dışı kaldığında ilgili talep noktalarının hangi alternatif tesislerden hizmet alacağı kararını da verebilecek şekilde düzenlenmiştir.

2. KRİTİK TESİSLER İÇİN SALDIRAN VE SAVUNANIN OLDUĞU YASAKLAMA/KORUMA PROBLEMLERİ VE İLGİLİ LİTERATÜR
(INTERDICTION/PROTECTION PROBLEM TYPES THAT INCLUDED ATTACKER AND DEFENSIVE FOR CRITICAL FACILITIES, RELATED LITERATURE)

Literatürdeki yayınlar incelendiğinde, yukarıda belirtildiği gibi bu problemlerin iki şekilde ele alındığı görülmektedir. Bunlardan biri yasaklamayı yapan (saldırgan) tarafından problemlerin ele alındığı modellerdir, bu modelleri, yasaklama modelleri olarak adlandıracağız. Diğeri ise korunacak tesisleri belirleyen savunucu tarafından ele alınan modellerdir ve bu modellere de koruma modelleri diyeceğiz. İki bakış açısının temel farkı modellerde eniyilenmeye çalışılan eğer saldırganın amacı ise modelin yasaklama modeli, eniyilenmeye çalışılan savunanın amacı ise koruma modeli olduğudur.

Literatürde öncelikle ağ yasaklama modellerinin çalışıldığı görülmektedir. Ağ yasaklama modellerinde tesis ile talep noktası arasındaki bağlantıların (arkların) kesilmesi/korunması ile en kısa yolun enbüyüklenmesi/enküçüklenmesi hedeflenir. Wollmer [3] makalesi bu alandaki ilk çalışmadır, çalışmada ağların (düğümler arası arkların) kesintiye uğraması modellenmiştir. Arkların kesintiye uğratılması ile akış kapasitesini düşürmek ve tesis ile talep noktası arasındaki en kısa mesafeyi enbüyüklemek amaçlanmıştır. Israeli [4] çalışmasında en kısa yol problemlerinde en kısa yolun en büyüklenmesini amaçlayan bir model ve çözüm önerisi sunmuştur ve problemi saldırgan açısından ele almıştır. Bu tür modellerde savunmacının ve saldırganın amaçlarına örnekler ise Tablo 2'deki gibi verilebilir.

Bu modellerin, düşman akışlarını aksatıcı uygulamalar [9], bulaşıcı hastalıkların kontrolü [10], terörle mücadele [11], kaçakçılığın engellenmesi [12] ve nükleer materyallerin kaçakçılığının durdurulması [13], sınır güvenliğinin sağlanması ve acil durum tesislerinin konumlandırılması [14] gibi çeşitli uygulamalarda kullanıldığı görülmektedir [15].

Tesis yasaklama/koruma modelleri ise belirli bir ağdaki en hayati tesislerin tahrip edilmesine odaklanır [16]. Yasaklama/koruma problemlerinde önceleri savaşlarda tedarik yollarının kesilmesine (ağ odaklı) yönelik konularda çalışılırken, son yıllarda kritik altyapılara yönelik (tesis odaklı) problemler de ele alınmaktadır [17]. Tesis yasaklama/koruma modellerinde de sistemi savunan ve bu sisteme zarar vermek isteyen bir saldırgan bulunur. Sistemi savunan, sunulan hizmetlerin eniyi şekilde sağlanmasını ve sürekliliğini, sisteme zarar vermek isteyen saldırgan ise en fazla zararı vermeyi amaçlar. Tesis yasaklama alanındaki ilk çalışma Church vd. [17]'nin çalışmasıdır. Bu çalışmada saldırganın bakış açısından problem ele alınmıştır ve RIM ve RIC olarak isimlendirilen iki model sunulmuştur. Ayrıca Scaparra ve Church [2] yasaklamanın etkilerini enküçükleyecek ve tahkimi eniyileyecek şekilde bir tamsayılı doğrusal program önermişlerdir. Bu model RIMF olarak adlandırılan iki seviyeli bir modeldir. Bu makalede yasaklamanın etkilerini azaltmak için mevcut tesislerin güçlendirilmesi ve böylece güvenliğin arttırılması amaçlanmıştır. Savunucu p kadar tesisten belli miktarını koruyabilir. Saldırgan ise korunmayan r kadar tesise saldırarak sistemin etkinliğini en yüksek oranda azaltmaya çalışır.

Stachelberg'in oyun teorisi (DA) (savunan (defender)-saldıran (attacker)) olarak ele alınan problemler; (DA) ve (AD) (saldırgan-savunan) şeklinde iki ve/veya (DAD) (savunan-saldırgan-savunan) şeklinde üç seviyeli olarak modellenmiştir.

Salmeron vd. [18], Salmeron ve Wood [19]'un çalışmaları elektrik şebekelerine yöneliktir. Salmeron vd. [18], elektrik şebekesine yapılan bir atak karşısında kritik olan bileşenlerin tanımlanması amaçlanmaktadır. Aksen ve Aras [20] çalışmalarında şarj istasyonlarının korunma planı ele alınmıştır. Losada vd. [21]'de oluşturulan modelde zaman periyotları göz önüne alınırken, Losada vd. [22] 'de ise tesis kapasitelerinin kısıtlı olduğu ancak talebin dış kaynaklardan da karşılanmasına izin verildiği varsayımında, zarar gören tesislerin tekrar kullanımları ve bu tesislerin düzelme süreleri modele dahil etmiştir. Aksen vd. [23] 'de saldırgan hizmet kesintisini enbüyüklemek istemektedir ve savunmacı (takipçisi) ise tüm müşterilerin talebini karşılamaktan sorumludur. Bu çalışmalar ve Lezama vd. [24] saldıran-savunan şeklinde iki seviyeli yasaklama modelleri olarak modellenmiştir. Forghani vd. [25]'de saldırgan-savunan şeklinde iki seviyeli bir model önerilmiştir, modelde saldırı sonrası müşteri ihtiyaçları kalan kaynaklardan ve dış kaynak kullanımı ile karşılanmaktadır. Müşteri ihtiyaçlarının karşılanmaması ile dış kaynak kullanımında ki müşteri memnuniyeti maliyetleri arasında bir karşılaştırma yapılmaktadır.

Wu ve Conejo [26], Alguacil vd. [27] ve Jian vd [28] çalışmalarında ise problemler üç seviyeli olarak modellenmiştir. Wu ve Conejo [26] ve Alguacil vd. [27]' yaptıkları çalışmalarda elektrik şebekelerinin savunması

Tablo 2. Ağ Yasaklama/Koruma Modellerinde Savunan ve Saldıran Açılarından Amaçlar
(Goals from Defending and Attacking Point of View on Network Interdiction/Protection models)

Savunmacı Açısından Amaçlar	Saldırgan Açısından Amaçlar
Ağdan mümkün olan en kısa sürede geçmek, [5].	En kısa yolun uzunluğunu enbüyüklemek, [4].
Ağdan geçen akış miktarını enbüyüklemek [6].	Ağdaki en büyük akışı en aza indirmek [3]
Ağ üzerinde yakalanmadan hareket etmek [7, 8].	Ağdaki bileşenlerin tespit olasılığını en üst düzeye çıkarmak [9]

problemi için üst seviye savunma planlamacısı, orta seviye saldırıyı yapanın seviyesi, alt seviye ise sistem operatörü olacak şekilde modellenmiştir. Jian vd. [28] yaptıkları çalışmada kentsel demiryolu ağına yönelik saldırılara karşı eniyi korumayı sağlamaya yönelik bir model geliştirmiştir. Üç seviyeli modellerde son seviye, savunan ve saldırganın sistemde oluşturdukları durum karşısında çözümü eniyilemek üzere değişikliğin yapıldığı bir aşamadır. Elektrik sistemlerinde sistem operatörü bu değişikliği yaparken demir yolarında ise yolcu verdiği kararlar ile son değişikliği yapmaktadır. Tesis yasaklama/koruma problemlerinin Tablo 3'te görüldüğü gibi iki ve üç seviyeli olarak modellendikleri görülmektedir. Ele alınan problemlerin bu modeller ile çözümünde ise matematiksel model, tam sayım gibi kesin çözüm yöntemleri kullanıldığı gibi daha büyük problemler için ise sezgisel yaklaşımlar da sıklıkla yer almaktadır.

Kesin çözüm algoritmalarında genellikle tam sayım ve Benders Ayrıştırma algoritmalarının kullanıldığı görülmektedir. Tam sayım algoritması, sınırlı sayıda düğüm değerlendirmesi ile eniyilemeyi garanti eden sistematik bir arama sağlar [27]. Losade [21] ise ayrıştırma metotlarının kullanıldığı iki adet çözüm yaklaşımı geliştirmiştir. İlki SVI'i temel alan ayrıştırma yaklaşımıdır. İkinci metot Benders Ayrıştırmasıdır. Wu ve Conejo [26] yaptığı çalışmada elektrik şebekelerinin savunması problemi için geliştirilen üç seviyeli bir modelde alt ve orta seviye birleştirilerek bir enbüyükleme problemi elde edilmiştir burada Benders Algoritmasından ve ikilinden yararlanılmıştır. Sezgisellerde ise yerel arama, tabu arama gibi yöntemlerin kullanıldığı görülmektedir. Lezame vd. [24]'de yerel arama ile problem çözülmüştür ve sonuçlar Genetik Algoritma (GA) ile karşılaştırılmıştır. Ayrıca Salmeron vd. [19] Benders tabanlı sezgisel modeller geliştirmişlerdir. Xiao vd. [32] yine RIMF modelini temel alarak iki amaçlı karma tamsayılı bir model oluşturulmuştur ve model dinamik yinelemeli kısmi optimizasyon sezgiseli ile çözülmüştür. Xiao vd. [32] 'nun çalışması gibi Salmeron [33] da üst seviyede ve alt seviyede, çelişen hedeflere sahip iki amaçlı modeller geliştirmişlerdir. Benzer şekilde Bölüm 3'de sunulan modeller de bu yapıya uymaktadır.

Literatürde yapılan çalışmalar bu konulara ilginin olduğunu göstermektedir. Çalışmaların %79,6'sının 2010 yılı sonrası yapıldığı görülmektedir. Problemlerin farklı yönleriyle ele alındığı ve gerçek hayat problemlerini daha iyi açıklayabilmek için çeşitli iyileştirmeler ile modellerin geliştirildiği ve çeşitlendirildiği görülmektedir. Aksen [34], RIMF [2] modelini temel alarak kapasite genişletme maliyetini modele dahil etmiştir. Korunacak tesislerin sayısını ise bütçe kısıtı ile belirlemiştir. Keçici [35] yeni tesis açma maliyeti, yer değiştirme maliyeti ve koruma maliyetlerini göz önüne almıştır, sınırlı bir bütçe ile saldırı

Tablo 3. Literatürde Yasaklama/Koruma Modellerinin Yıl, Model Karakteristikleri ve Çözüm Yaklaşımları
(Year, Model Characteristics and Solution Approaches of Interdiction/Protection Models in the Literature))

Yazar	Yıl	Model Seviyesi ve Türü	Çözüm Yöntemi
Salmeron vd. [18]	2004	2 (AD)	Sezgisel Algoritma (Benders Ayrıştırma)
Scaparra ve Church [2]	2008	2 (DA)	Tamsayımlama
Losade vd. [21]	2010	2 (DA)	(1) SVI (Super-Valid-Inequalities) Tabanlı Ayrıştırma (D-SVI) (2) Benders Ayrıştırması (D-Bend)
Aksen ve Aras [20]	2011	2 (DA)	(1) Yasaklı Arama (2) Konum ve Koruma Kararlarının Ayrıldığı Sıralı Yöntem
Losade vd. [22]	2012/a	2 (DA)	(1) D-Bend (2) D-SVI (3) D-Bend and D-SVI Melez Ayrıştırma Yöntemi
Losade vd. [29]	2012/b	2 (AD)	Matematiksel Model
Aksen vd. [23]	2013	2 (AD)	(1) İlerici Şebeke Arama Yöntemi (2) Sezgisel Algoritma (Simpleks Arama)
Alguacil vd. [27]	2014	3 (DAD)	Tamsayımlama
Salmeron ve Wood [19]	2015	2 (AD)	(1) Benders Ayrıştırması (2) Tamsayımlama
Jian vd. [28]	2015	3 (DAD)	Sezgisel Algoritma (Değişken Komşu Arama)
Wu ve Conejo [26]	2017	3 (DAD)	Yerel Arama
Lezama vd. [24]	2017	2 (AD)	Yerel Arama
Ghaffarinasaba ve Atayi [30]	2018	2 (DA)	Tamsayımlama
Ramamoorthy vd.[31]	2018	2 (AD)	Benders Ayrıştırması
Xiao vd.[32]	2020	2 (DA)	Sezgisel Algoritma (Dinamik Yinelemeli Kısmi Optimizasyon)

sonrası toplam hizmet kapsamını enbüyüklemek amaçlanmıştır. Zhu [36] RIMF modelini temel alarak, bir tesisin korunmuş olmasının, bir saldırıya karşı kesin olarak koruma sağlamayacağını ortaya koymuş ve koruma başarısını olasılıklı olarak modele dahil etmiştir. Losada vd. [21] ve Losada vd. [22]'de zarar gören tesislerin yeniden düzelme sürelerini modele dahil edilmiştir. Losada vd. [29] yaptığı çalışmada bozulma yoğunluk seviyelerinin belirsiz olduğunu göz önüne alarak stokastik bir yasaklama modeli önermiştir. Liberatore vd. [37] da RIMF modelini temel alarak, yasaklanacak tesis sayısının kesin olmayacağını göz önüne alarak stokastik bir problem tanımlamıştır. Aksen vd. [23] tesis kapasitesini ve dış kaynak kullanımını modele dahil etmişlerdir. Jian vd. [28] problemde koruma amacı ile ayrılan kaynakların etkinliğini ölçmeyi amaçlamıştır.

3. ÖNERİLEN MODELLER (PROPOSED MODELS)

Önceki çalışmalar göz önüne alındığında saldırı tipinin belli bir sayıda ve tek tip olacağının varsayıldığı, saldırı tiplerinin ve koruma tiplerinin de farklı olabileceğinin göz önüne alınmadığı görülmektedir. Gerçek hayat problemlerine bakıldığında saldırı tipinin ve bu saldırıya karşı alınan önlemin tek tip olmayabileceği açıktır. Örneğin bir terörist gurubun bir tesisi hedef alarak yapabileceği birbirinden tamamen farklı saldırı tipleri mevcuttur. Günümüzdeki teknolojik gelişmeler de bu çeşitliliği arttırmaktadır. Bir tesise canlı bomba, bombalı araç veya drone ile ya da uzaktan roket atışı veya siber saldırılar vb. ile saldırılabilir. Aynı şekilde bu saldırılara karşı alınacak önlemler de bağlı olarak birbirinden farklı olabilmektedir ve her biri farklı maliyetlere de sahiptir. Bu çalışma çerçevesinde öncelikle saldırı ve koruma yöntemlerinin tek tip olmayacakları, yanı sıra bazı koruma şekillerinin birden fazla saldırı tipini de önleyebileceği göz önüne alınmıştır. Yine yapılan çalışmaların bir kısmında hizmet sağlayan tesislerin kapasitelerinin sınırsız olduğu ya da kapasitesinin arttırılabileceği varsayılmaktadır. Önerilen ikinci modelde ise hizmet sağlayan tesislerin bir kapasitesinin olduğu gerçekliği modele dahil edilmiştir ve saldırganın, kapasite ile talep arasındaki dengeyi bozmayı öncelikle hedefleyeceği göz önüne alınmıştır. Terör guruplarının hizmetleri kesintiye uğratma amacı ile yaptıkları tesis saldırılarına bakıldığında öncelikli amacın tesise zarar vermekten çok toplum üzerinde infial yaratmak olduğu görülmektedir. Bu amaç, önerilen ikinci modele eklenmiştir. Bu yeni amaçla birlikte Scaparra ve Church [2]'de sınırsız kapasite varsayımı ile sunulan iki seviyeli RIMF modeli, sınırlı kapasiteli ve saldırı savunma tipleri göz önüne alınarak revize edilmiştir. İzleyen bölümde bu modeller verilmektedir.

3.1. İki Seviyeli Çoklu Saldırı Tipli Yasaklama/Koruma Modeli (R_eIMF)

(Bi-Level Multi Attack Type Interdiction/Protection Model (R_eIMF))

Bu çalışmada genel olarak hizmet sunan bir tesis (kritik tesis) ve müşterinin (talep noktası) olduğu, tesisin yasaklanma/korunma durumunun göz önüne alındığı bir model önerilmiştir. Her hizmet türünün özel kısıtları olmakla birlikte, burada açıklananlar, doğalgaz sistemleri, silah depoları, acil servisler, ticari tesisler, elektrik şebekeleri, su sistemleri vb. hizmet sunan ve bu hizmeti alan müşterilerin olduğu tüm sistemler için geçerli olacaktır.

Çözmeyi amaçladığımız problemde kritik tesisler aracılığı ile belirli bir bölgeye (talep noktası) hizmet sunulmaktadır. Sunulan hizmetin önemi nedeni ile talep noktalarının ihtiyacı olan hizmet kesintisiz olarak sunulmalıdır. Kritik tesislere yapılan saldırılar ile bu noktalara sunulan hizmet kesintiye uğrayabilir. Saldırganların kritik tesisleri hedef almaları ve bunlardan yeterli korunmaya sahip olmayanlarını devre dışı bırakacakları göz önüne alınacaktır. Kritik tesisin faaliyetlerini yerine getiremeyecek şekilde devre dışı bırakılması, durdurulması yasaklama olarak ele alınacaktır.

Bu makalede Scaparra ve Church [2]'ın RIMF modeli temel alınarak iki seviyeli bir matematiksel model geliştirilmiş ve R_eIMF olarak isimlendirilmiştir. r ile verilen değer yasaklanabilecek tesis sayısını ifade ederken re ile verilen değer e tipi yasaklama ile yasaklanabilecek tesis sayısını vermektedir. Literatürde, Aksen ve Aras [20], Aksen vd. [23], Xiao vd. [32], Salmeron [33] ve Liberatore vd. [37] başta olmak üzere pek çalışmada RIMF[2] modeli temel alınarak yeni modeller geliştirilmiştir.

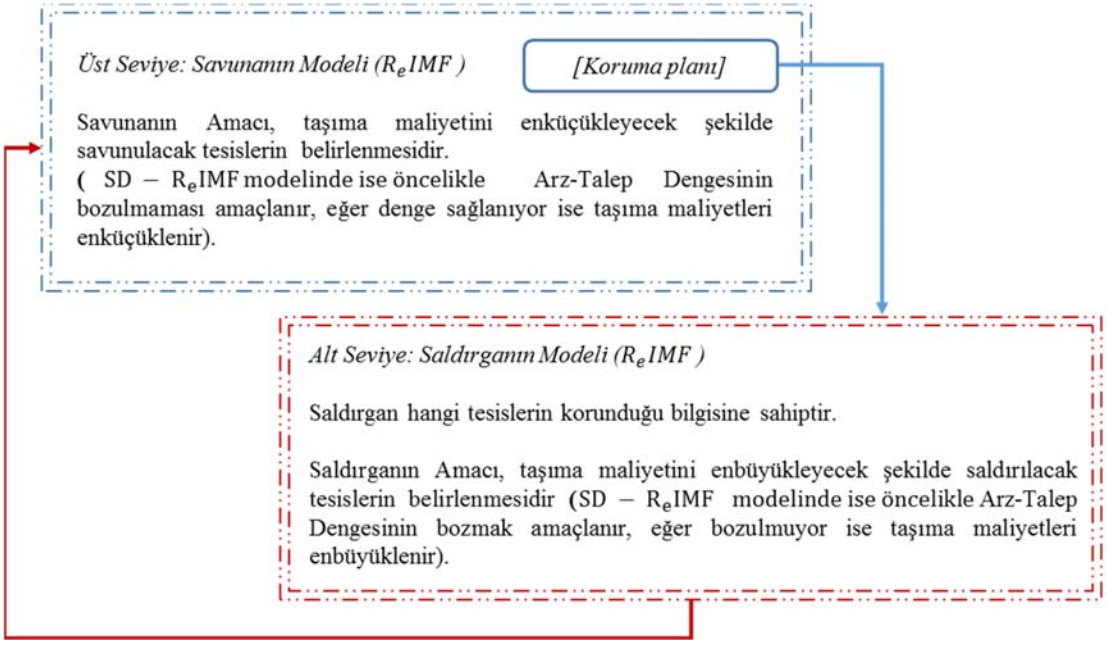
Geliştirilen R_eIMF modeli iki seviyeli bir modeldir ve bu yeni modelin üst seviyesi savunan seviyesidir ve koruma planı üretecek olan seviyedir. Alt seviye ise saldırganın seviyesidir. Saldırgan nerelerin korunduğu bilgisine sahiptir ve saldırı planlarını buna göre yapmaktadır. Stackelberg oyun teorisine [1] dayanan bu model Şekil 1'de görüldüğü gibi savunan-saldıran (DA Defender-Attacker) şeklinde oluşturulmuştur.

R_eIMF modelinin varsayımları şu şekildedir:

a) Saldırgan, farklı tiplerde ve belirli sayılarda saldırı yapabilme yeteneği ve donanımına sahiptir ve bu savunma planlamacısı tarafından bu bilinmektedir.
b) Saldırgan saldırı anında (a)'da belirtilen saldırı tiplerinin belli sayıdaki bir karmasını kullanacaktır.
c) Saldırgan hangi tesislerin korunduğunu bilmektedir.
d) Saldırganın farklı çeşitteki saldırı tiplerinde kaçar saldırı yapabilme kabiliyetine sahip olduğu bilinmektedir.
e) Bir saldırı periyodunda saldırganın (d)'de belirtilen saldırılarından toplamda kaç adedini yapabileceği bilinmektedir.
f) Saldırgan hangi tesislerin hangi saldırı tiplerine karşı korunduğunu bilmektedir ve bu tesislere ilgili saldırı tipi ile saldırmaz.
g) Bir tesis yasaklandığında hizmet alınacak alternatif fakat daha yüksek maliyetli bir tesis her zaman vardır.

İndisler:

$i \in I$: Talep noktası
$j \in J$: Kritik tesis
$e \in E$: Saldırı tipi
$f \in F$: Koruma tipi



Şekil 1. İki Seviyeli Yeni R_eIMF ve SD − R_eIMF Koruma Modelleri (Bi-level New R_eIMF and SD − R_eIMF Protection Models)

Kümeler
I : Talep noktaları I= {i | i=1,2,..n}
J : Kritik tesisler J= {j | j=1,2,..p}
E : Saldırı tipleri E= {e | e=1,2,..g}
F : Koruma tipleri F= {f | f=1,2,..t}

Parametreler:
d_{ij} : Kritik tesis j'den talep noktası i'ye sunulan hizmetin birim maliyeti
a_i : i. talep noktasının talebi
b_{jf} : j kritik tesisinin f koruma tipi ile tahkim (korunma) maliyeti
b_{tot} : Savunma için ayrılan toplam bütçe
R : Saldırganların yasaklayabileceği kritik tesis sayısı
r_e : Saldırganın e.saldırı tipinde yapabileceği yasaklama sayısı.
L_{ijk} : k kritik tesisinin, i talep noktasına olan mesafesi, j kritik tesisinin i talep noktasına olan mesafesinden büyükse 1, eşit veya küçükse 0'dır.
K_{ef} : e saldırı tipi f koruma tipi ile korunabiliyor ise 1, korunamıyor ise 0 değerini almaktadır.

Karar Değişkenleri;

$$z_{jf} = \begin{cases} 1, & j\ kritik\ tesisi\ f\ koruma\ tipi\ ile\ korunursa \\ 0, & d.d. \end{cases}$$

$$s_{je} = \begin{cases} 1, & j\ kritik\ tesisi\ e\ saldırı\ tipi\ ile\ yasaklanırsa \\ 0, & d.d. \end{cases}$$

$$x_{ij} = \begin{cases} 1, yasaklama\ sonrası\ i\ talep\ noktası \\ \quad j\ kritik\ tesisinden\ hizmet\ alırsa \\ 0, & d.d. \end{cases}$$

Amaç Fonksiyonu

$$\text{enk}\, H(z) \tag{1}$$

kısıtları altında

$$\sum_{j\in J}\sum_{f\in F} b_{jf} z_{jf} \le b_{tot} \tag{2}$$

$$z_{jf} \in \{0,1\} \quad \forall j \in J, \forall f \in F \tag{3}$$

öyle ki

$$H(z) = \text{enb} \sum_{i\in I}\sum_{j\in J} a_i d_{ij} x_{ij} \tag{4}$$

kısıtları altında

$$\sum_{j\in J} x_{ij} = 1 \qquad \forall i \in I \tag{5}$$

$$\sum_{j\in J} s_{je} \le r_e \qquad \forall e \in E \tag{6}$$

$$\sum_{j\in J}\sum_{e\in E} s_{je} = R \tag{7}$$

$$s_{je} \le 1 - K_{ef} . z_{jf} \qquad \forall j \in J, \forall e \in E, \forall f \in F \tag{8}$$

$$\sum_k L_{ijk} . x_{ik} \le \sum_e s_{je} \qquad \forall j \in J, \quad \forall i \in I \tag{9}$$

$$\sum_i x_{ij} \le n - n . s_{je} \qquad \forall j \in J, \quad \forall e \in E, \forall i \in I \tag{10}$$

$$s_{je} \in \{0,1\} \qquad \forall j \in J, \forall e \in E \tag{11}$$

$$x_{ij} \in \{0,1\} \qquad \forall i \in I, \forall j \in J \tag{12}$$

Aşağıda R_eIMF modelinin kısıtları sırasıyla açıklanmaktadır:

Eş. 1 İki seviyeli modelin üst seviye amaç fonksiyonudur. p kadar tesisten r kadarı yasaklandığında ağırlıklı maliyeti enküçüklemeyi amaçlar.
Eş. 2 p kadar tesisten savunma için ayrılmış olan bütçe kadar tesise tahkim yapılmasını sağlar.
Eş. 4 İki seviyeli modelin alt seviye amaç fonksiyonudur. p kadar tesisten r kadarı yasaklandığında ağırlıklı maliyeti enbüyüklemeyi amaçlar.
Eş. 5 Her talep noktasının saldırı sonrası bir tesisten hizmet almasını sağlar.
Eş. 6 e saldırı tipi ile en fazla yasaklanabilecek tesis sayısını sınırlar.
Eş. 7 R kadar tesisin yasaklanmasını sağlar.
Eş. 8 Korunan bir tesisin yasaklanmasını önler.
Eş. 9 Yasaklama sonrası, yasaklı bir tesise talep noktasının atanmasını önler. Yasaklama sonrası yasaklanan tesisten sonraki en yakın tesise i talep noktasının atanmasını sağlar.

"L_{ijk} parametresi RIMF [2] modelinde ($T_{ij} = \{k \in J \text{ I } k \neq j \; ve \; d_{ik} > d_{ij}\} T_{ij}$, j kritik tesisi dışında kalan mevcut kritik tesislerin setidir ve bu küme içindeki tüm kritik tesislerin i kritik tesisine hizmet sunma maliyeti, j kritik tesisinin i talep noktasına hizmet sunma maliyetinden fazladır) olarak açıklanan T_{ij} parametresi yerine ilave edilmiştir ve eğer bir tesis yasaklanırsa o tesisten hizmet alan talep noktasının en yakın tesisten hizmet almasını sağlayan Eş. 9 kısıtı bu değişiklik göz önüne alınarak revize edilmiş ve Eş. 10 oluşturulmuştur".

Eş. 10 no.lu kısıt ise yeni bir kısıttır. Bu kısıt ise eğer bir j santrali herhangi bir e saldırı tipi ile yasaklanırsa o tesisten hizmet alınmasını engellemektedir.
Eş. 3, Eş. 11 ve Eş. 12 işaret kısıtlarıdır.

3.2. Arz Talep Dengesi Bozma Amaçlı İki Seviyeli Çoklu Saldırı Tipli Koruma Modeli ($SD - R_eIMF$)

(Bi-Level Multi Attack Type Interdiction/Protection Model that Aiming to Disrupt the Supply-Demand Balance ($SD - R_eIMF$))

Kritik tesislerden sunulan hizmet, talep noktalarına iletilmektedir. Bu tesislerden bazıları sistem dışı kaldığında kalan tesisler talep noktalarının ihtiyaçlarını farklı maliyetlerle karşılamaya devam ederler.

R_eIMF modelinde kritik tesislerin kapasitelerinin sınırsız olduğu varsayılmaktadır. Gerçekte ise her tesisin bir kapasitesi vardır. Saldırgan tarafından gerçekleştirilen yasaklamalar ile geriye kalan, yasaklanamayan tesislerin kapasiteleri toplamı, talebi karşılamaya yetmeyebilir. Saldıranın bu durumda iki amacı vardır. İlk amacı klasik r-yasaklama modellerinde olduğu gibi saldırı sonrası, taleplerin en yüksek maliyetle karşılanmasına sebebiyet vermek, diğer amacı ise yaptığı saldırılar ile talebi karşılanamayan noktalar oluşturmaktır. Bu durum bazı bölgelerin hizmet alamaz duruma gelmesine sebep olacaktır. Nitekim talebin en yüksek maliyetle karşılanması durumu da, izleyen en uygun noktadan talep alma zorunluluğu sebebiyle ortaya çıkacaktır. Terörizm belirli amaçlar için bir araç olarak kamunun provoke edilmesi, topluma korku salma ve yıldırmak amacıyla tasarlanan eylemlerin kasıtlı ve sistematik kullanımı olarak tanımlanmaktadır. Terör saldırılarında, toplum üzerinde büyük bir infial yaratma hedefi vardır. Bu açıdan ele aldığımızda bir terör saldırısında öncelikle arz talep dengesizliğini oluşturmak daha cazip görülmektedir. Bu bağlamda modele saldırganın öncelikle arz talep dengesizliğine en fazla sebep olacak şekilde saldırılarını organize edeceği gerçeği eklenmek istenmiştir. Saldırgan eğer böyle bir dengesizliğe sebep olabiliyor ise önce bunu tercih edecektir. Ancak olamıyorsa maliyeti en fazla oluşturacak şekilde saldıracaktır. Aşağıda bu durumun göz önüne alındığı $SD - R_e$IMF yeni modeli, R_eIMF modelinden farklı olan varsayım ve model bileşenleri ile birlikte verilmektedir.

Varsayımlar:

a) Bir tesis yasaklandığında hizmet alınacak alternatif bir tesis her zaman mevcut değildir. Tesislerin kapasiteleri kısıtlıdır.
b) Saldırgan öncelikle tesislerin kapasitesini talep miktarının altına düşürmeyi amaçlar, bunu yapamaz ise maliyeti enbüyüklemeyi hedefler.

Parametreler;

$tkap_j$: j kritik tesisinin kapasitesi
toptalep : Korunması planlanan bölgenin ihtiyacı olan toplam talep miktarı

Karar Değişkenleri;

$$S_j = \begin{cases} 1, & j \; kritik \; tesisi \; yasaklanırsa \\ 0, & d.d. \end{cases}$$

$$y = \begin{cases} 1, & yasaklama \; sonrası \; kalan \\ & toplam \; kapasite \; yetersiz \; ise \\ 0, & d.d. \end{cases}$$

Amaç Fonksiyonu

$$\text{enk } H(z) \tag{13}$$

Kısıtları altında

$$\sum_{j \in J} \sum_{f \in F} b_{jf} z_{jf} \leq b_{tot} \tag{14}$$

$$z_{jf} \in \{0,1\} \quad \forall j \in J, \; \forall f \in F \tag{15}$$

öyle ki

$$H(z) = \text{enb} \sum_{i \in I} \sum_{j \in J} a_i d_{ij} x_{ij} + M.y \tag{16}$$

kısıtları altında

$$\sum_{j \in J} x_{ij} \leq 1 \qquad \forall i \in I \tag{17}$$

$$\sum_{j \in J} x_{ij} \geq 1 - y \qquad \forall i \in I \tag{18}$$

$$\sum_{j \in J} s_{je} \leq r_e \qquad \forall e \in E \tag{19}$$

$$\sum_{j\in J}\sum_{e\in E} s_{je} = R \quad (20)$$

$$s_{je} \leq 1 - K_{ef} \cdot z_{jf} \qquad \forall j \in J,\ \forall e \in E,\ \forall f \in F \quad (21)$$

$$\sum_k L_{ijk} \cdot x_{ik} \leq S_j \qquad \forall j \in J,\ \forall i \in I \quad (22)$$

$$\sum_{i\in I} a_i = toptalep \quad (23)$$

$$\frac{\sum_e s_{je}}{1+\sum_e s_{je}} + \frac{1}{2} \geq S_j \geq \frac{\sum_e s_{je}}{1+\sum_e s_{je}} \qquad \forall j \in J \quad (24)$$

$$\sum_{j\in J} tkap_j - \sum_{j\in J} S_j * tkap_j < toptalep + M(1-y) \quad (25)$$

$$\sum_{j\in J} tkap_j - \sum_{j\in J} S_j * tkap_j \geq toptalep - M.y \quad (26)$$

$$s_{je} \in \{0,1\} \qquad \forall j \in J, \forall e \in E \quad (27)$$

$$x_{ij} \in \{0,1\} \qquad \forall i \in I, \forall j \in J \quad (28)$$

$$y \in \{0,1\} \quad (29)$$

Yukarıda verilen SD – R_eIMF modeline y değişkeni eklenmiştir. Eğer saldırgan elindeki kaynaklar ile tesislerin sunduğu hizmeti talep miktarının altına düşürebilirse y=1 değerini alır. Saldırganın öncelikli amacı budur. Saldırgan tesis kapasitesini talep miktarının altına düşüremiyorsa y=0 olur ve amaç fonksiyonu ağırlıklı maliyeti enbüklemeyi amaçlar.

Eş. 13 İki seviyeli modelin üst seviye amaç fonksiyonudur. Öncelikle arz miktarının talep miktarının altına düşmemesini amaçlar, bu sağlandığında, p kadar tesisten r kadarı yasaklandığında ağırlıklı maliyet enküçüklenecektir.

Eş. 14 p kadar tesisten savunma için ayrılmış olan bütçenin yeteceği kadar tesise tahkim yapılmasını sağlar.

Eş. 16 İki seviyeli modelin alt seviye amaç fonksiyonudur. Öncelikle arz miktarının talep miktarının altına düşmesini amaçlar, bu sağlanamaz ise p kadar tesisten r kadarı yasaklandığında ağırlıklı maliyeti enbüyüklemeyi amaçlar.

Eş. 17 Her talep noktasının saldırı sonrası en fazla bir tesisten hizmet almasını sağlar.

Eş. 18 Saldırı sonrası eğer tesis yeterli ise her talep noktasının bir tesisten hizmet almasını sağlar. Eğer kapasite yetersiz ise i. talep noktasının talebi karşılanmayabilir.

Eş. 19 e saldırı tipi ile en fazla yasaklanabilecek tesis sayısını sınırlar.

Eş. 20 R kadar tesisin yasaklanmasını sağlar.

Eş. 21 Korunan bir tesisin yasaklanmasını önler.

Eş. 22 Yasaklama sonrası, yasaklı bir tesise talep noktasının atanmasını önler. Yasaklama sonrası yasaklanan tesisten sonraki en yakın tesise, talep noktasının atanmasını sağlar.

Eş. 23 Toplam talebin değerini belirler.

Eş. 24 Bir tesisin yasaklı olup olmadığını belirler

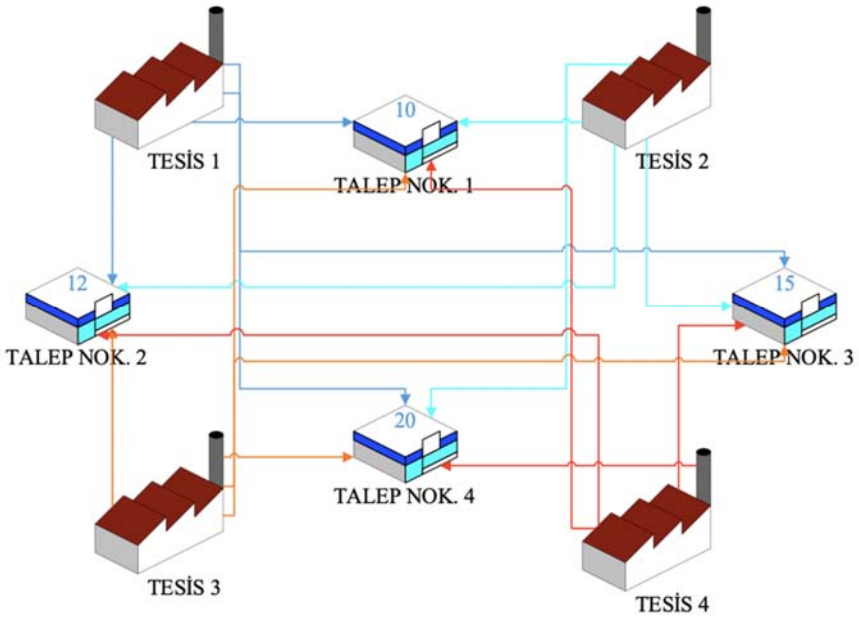
Eş. 25 ve Eş. 26 saldırı sonrası kalan tesislerin toplam kapasitesi, toplam talepten az ise y = 1, diğer durumda y = 0 olmasını sağlar.

Eş. 15, Eş. 27, Eş. 28 ve Eş. 29 karar değişkenlerinin işaret kısıtlarıdır.

4. UYGULAMA (CASE STUDY)

Bu bölümde modelleri test etmek için hizmet sunan dört kritik tesis (*j*), hizmet alan dört talep merkezi (*i*) ve iki farklı yasaklama (*e*) ve karşılık gelen iki farklı koruma tipinin (*f*) olduğu bir test problemi kullanılmıştır ve talep miktarları (a_i) Şekil 2'de görülmektedir. Koruma kaynağı beş, saldırı kaynağı ise iki olarak alınmıştır.

Modeller askeri ve kritik tesisler göz önüne alınarak tasarlanmıştır. Gerçek veri setlerine ulaşmak, özellikle



Şekil 2. Dört tesis ve dört talep noktasından oluşan örnek problemin şematik gösterimi
(Schematic representation of the sample problem consisting of four facilities and four demand points)

konunun güvenlik ile ilgili olması nedeni ile güçtür. Bu sebeple veri türetme zorunluluğu bulunmaktadır.

Probleme ilişkin türetilen parametreler Tablo 4, Tablo 5 ve Tablo 7'de verilmiştir.

Kritik tesis (j)'nin yasaklanması sonrası hizmet alınabilecek, kendisinden daha uzak mesafeli kritik tesisleri (k) gösteren L_{ijk} katsayı seti Tablo 5'de verilmiştir. Bu katsayı değerleri, (i) talep noktasının (k) tesisine olan mesafesi, (j) tesisine olan mesafesine eşit ya da daha uzak mesafede ise 1, diğer durumda 0 değerini alır.

Bölüm 3.1'de verilen bu matematiksel modele dikkate edilirse, amaç fonksiyonu *Enk (Enb*) yapısındadır, bir başka deyişle saldıran, bir maliyet fonksiyonunu, H(z), enbüyüklemeye, savunan ise aynı fonksiyonu enküçüklemeye çalışmaktadır. Bu çerçevede saldıran, öyle kritik tesislerin yasaklanmasını hedefler ki, talep noktalarının (i) olabildiğinde uzak (büyük dij'ler) kritik tesislerden (j) hizmet alması, böylece bir maliyet fonksiyonunun enbüyüklenmesi amaçtır. Savunan ise üst model ile aynı fonksiyonu enküçüklemeyi, talep noktalarının olabildiğince yakın (küçük dij'ler) kritik tesislerden hizmet alabilmesini isteyecektir. Bu *Enk (Enb*) yapı nedeniyle model doğrusal değildir. Literatürde bu problemler daha önce de belirtildiği gibi Savunan-Saldıran tipinde yer almıştır. Bu problemlerin çok amaçlı olarak ele alındığı Xiao vd. [32] ve Salmeron [33] görülmektedir. Ancak özellikle ε kısıt vb. yöntemlerden yararlanarak bazı amaçların yerine geçebilecek kısıtların probleme eklenmesi düşünülebilir. Öte yandan gerçek veri bulmanın mümkün olması halinde bile, saldırı ve savunma tipleri, savunma sistemlerinin yarattığı maliyetler ve bu sistemlerdeki gizlilik sebebiyle büyük sayılarda olmayacaktır. Bu durumda bu modeller günümüzde karşılaşılan diğer matematiksel modellere göre daha küçük boyutlu olabilmektedir. Bu açıklamalar ışığı altında aşağıda, modelin ilk seviyesine karşı gelen savunma planları modele verilerek, ikinci seviye çözümüne ilişkin işlemler açıklanmaktadır.

Verilen örnek problemde kritik tesislerin kapasitelerinin sınırsız olarak kabul edildiği R_eIMF modeli ile elde edilen çözüm sonucu Tablo 6'da verilmiştir. Problemde, verilen parametreler için ortaya çıkan farklı savunma planları (koruma kombinasyonları) modelin ilk seviyesine karşılık gelmek üzere girdi olarak verildiğinde her çalıştırmada o savunma planı için eniyi saldırı planı bulunmuştur. Modelin ikinci seviyesi GAMS programı ile çalıştırılmaktadır. Örnek problemde, alt seviye model tüm savunma planları için çözüldüğünde, Tablo 6'da verilen dört savunma kombinasyonunun aynı eniyi amaç fonksiyonu değerini (742 pb) verdiği görülmektedir. Tanımlanan problemin savunan odaklı olduğu düşünülürse, saldırganın gerçekleştirebileceği saldırı planlarından, en az zararı verebildiği savunma planları, savunan için en iyi çözüme karşı gelmiş olacaktır. Tablo 6'da sadece eniyi çözüme karşı gelen sonuçlar yer

Tablo 4. Kritik Tesisler (j) ile Talep Merkezleri (i) arası mesafeler ve talep merkezleri talep miktarları
(Distances From Critical Facilities to Demand Pointies, and Demand Pointies's Demand Quantities)

j / i	1	2	3	4	Talep (a_i)
1	12 km	11 km	11 km	10 km	10 adet
2	16 km	17 km	19 km	18 km	12 adet
3	20 km	22 km	16 km	21 km	15 adet
4	10 km	21 km	10 km	15 km	20 adet

Tablo 5. L_{ijk} Katsayılar Matrisi (L_{ijk} coefficient matrix)

k / i, j	1	2	3	4
1.1	0	0	0	0
1.2	1	0	0	0
1.3	1	0	0	0
1.4	1	1	1	0
2.1	0	1	1	1
2.2	0	0	1	1
2.3	0	0	0	0
2.4	0	0	1	0
3.1	0	1	0	1
3.2	0	0	0	0
3.3	1	1	0	1
3.4	0	1	0	0
4.1	0	1	0	1
4.2	0	0	0	0
4.3	0	1	0	1
4.4	0	1	0	0

almaktadır. 1 no.lu koruma planında beş adet koruma kaynağının $z_{11}, z_{12}, z_{22}, z_{31}, z_{32}$ şeklinde tesislere atanarak koruduğu görülmektedir. Bu koruma planına göre 1 ve 3 no.lu tesisler, her iki saldırı tipine karşı korunmaktadır. Bu durum saldırganın 1 ve 3 no.lu tesislere saldırmasını engellemektedir. 2 no.lu tesis yalnızca 2 no.lu saldırı tipine karşı (z_{22}) korunmaktadır. 4 no.lu tesisin ise 1 ve 2 no.lu saldırı tiplerine karşı korunmadığı görülmektedir. Saldırgan sadece s_{21}, s_{42} saldırı planı ile 2 ve 4 no.lu tesislere saldırmıştır. Saldırgan iki adet saldırı kaynağını aynı tesise saldırmak için kullanmamış, hem 1 no.lu hem de 4 no.lu tesisi yasaklayacak şekilde saldırısını planlamıştır.

Plan 1'de verilen koruma planının, koruma ve saldırı planları sonucu olarak i talep noktaları x_{13}, x_{21}, x_{33}, x_{43} şeklinde hizmet almaya devam etmişlerdir. 1 no.lu talep noktası 3 no.lu tesisten (x_{13}), 2 no.lu talep noktası 1 no.lu tesisten (x_{21}), 3 no.lu talep noktası 3 no.lu tesisten (x_{33}), 4 no.lu talep noktası 3 no.lu tesisten (x_{43}) hizmet alarak 742 birimlik bir maliyet oluşmuştur.
Ayrıca en iyi amaç fonksiyonu değerini veren tüm koruma planları birlikte incelendiğinde özellikle 1 ve 3 no.lu tesisin, tüm koruma planlarında her iki saldırı tipine karşı da korunduğu görülmektedir ve böylece hangi tesislerin kritik olduğu konusunda model bilgi sağlamaktadır.

Arz talep dengesi bozmaya yönelik SD – R_eIMF modeli için ise Tablo 7'deki parametreler modele eklenmiştir (Tablo 7). Büyük M değeri 5000 olarak kabul edilmiştir. Tesislerin belirli bir kapasitesinin olduğunu göz önüne alan SD – R_eIMF modelinin çözüm sonuçları ise şu şekilde gerçekleşmiştir.

1 - 4 no.lu tesislerin birlikte korunduğu ve 3 - 4 no.lu tesislerin birlikte korunduğu durumlar için arz talep dengesinin sağlanamadığı görülmektedir. Ancak 1 - 2 , 1 - 3 , 2 - 3 ve 2 - 4 no.lu tesis çiftlerinin birlikte korunduğu koruma planlarında arz talep dengesinin korunduğu ve makul değerler aldığı Tablo 8'de görülmektedir. Bunlarda 1 - 3 no.lu tesisin birlikte korunduğu koruma planlarının ise en iyi amaç değerini (748) almaktadır.

SD – R_eIMF modelinin çözümü ile elde edilen eniyi amaç değerine sahip koruma planları Tablo 9'da verilmiştir. Buna göre yine 1 ve 3 no.lu tesislerin her iki saldırı tipine karşı korunduğu görülmektedir (z_{11} , z_{12} , z_{31} , z_{32}). Örnek problemde kapasite kısıtlarının göz önüne alınması sebebi ile elde tesis - talep merkezi eşleştirmelerine bakıldığında ise 2 no.lu talep merkezinin kapasite kısıtlarından kaynaklı olarak hem 1 no.lu hem de 3 no.lu tesisten hizmet aldığı görülmektedir (x_{21}, x_{23}).

Model öncelikle arz talep dengesini bozacak saldırıları engelleyecek şekilde koruma planlarını belirlemiş ve bu çerçevede en iyi amaç fonksiyonu değerini veren koruma planını seçmiştir.

Her iki modelin sonuçları birlikte değerlendirildiğinde: Önerilen ilk modelde, kapasitenin sınırsız olduğu varsayılmaktadır ve test problemi için eniyi amaç fonksiyonu değeri olan 742 pb. elde edilmiştir. İkinci modelde kapasite kısıtları göz önüne alınmaktadır ve test problemine "tesislerin kapasitesi (tkapj)" parametresi eklenmiştir. Bu yeni durum için ikinci model ile problem çözüldüğünde en

Tablo 6. R_eIMF Modeli İçin Amaç Fonksiyonu Değeri En İyi Olan Koruma Planları
(Optimum Protection Plans for R_eIMF model)

Plan No	H(z) (Para Birimi)	Korunan Tesisler z_{jf}	Yasaklanan Tesisler s_{je}	Yasaklama Sonrası Talep Noktalarının Hizmet Aldığı Tesisler x_{ij}
1	742 pb	$z_{11}, z_{12}, z_{22}, z_{31}, z_{32}$	s_{21}, s_{42}	$x_{13}, x_{21}, x_{33}, x_{43}$
2	742 pb	$z_{11}, z_{12}, z_{21}, z_{31}, z_{32}$	s_{22}, s_{41}	$x_{13}, x_{21}, x_{33}, x_{43}$
3	742 pb	$z_{11}, z_{12}, z_{31}, z_{32}, z_{41}$	s_{21}, s_{42}	$x_{13}, x_{21}, x_{33}, x_{43}$
4	742 pb	$z_{11}, z_{12}, z_{31}, z_{32}, z_{42}$	s_{22}, s_{41}	$x_{13}, x_{21}, x_{33}, x_{43}$

Tablo 7. Kritik tesislerin kapasiteleri ($tkap_j$) (Capacities of Critical Facilities ($tkap_j$))

j	1	2	3	4
Kapasite ($tkap_j$)	30 adet	40 adet	27 adet	25 adet

Tablo 8. Kapasite kısıtlı örnek problem için olası tüm çözüm alternatifleri
(All Possible Solution Alternatives for capacity limited sample)

Korunan Tesisler	Amaç Fonksiyonu Değerleri (Para Birimi)
1 ve 2 no.lu tesisler korunursa	834 pb
1 ve 3 no.lu tesisler korunursa	748 pb
1 ve 4 no.lu tesisler korunursa	Arz-Talep Dengesi Bozuk
2 ve 3 no.lu tesisler korunursa	844 pb
2 ve 4 no.lu tesisler korunursa	964 pb
3 ve 4 no.lu tesisler korunursa	Arz-Talep Dengesi Bozuk

Tablo 9. SD − R_eIMF Modeli İçin Amaç Fonksiyonu Değeri en iyi olan Koruma Planları
(Optimum Protection Plans for SD − R_eIMF model)

Plan No	H(z) (Para Birimi)	Korunan Tesisler z_{jf}	Yasaklanan Tesisler s_{je}	Yasaklama Sonrası Telep Noktalarının Hizmet Aldığı Tesisler x_{ij}
1	748 pb	z_{11} , z_{12} , z_{22} , z_{31} , z_{32}	s_{21} , s_{42}	x_{13}, x_{21}, x_{23}, x_{33}, x_{41}
2	748 pb	z_{11} , z_{12} , z_{21} , z_{31} , z_{32}	s_{22} , s_{41}	x_{13}, x_{21}, x_{23}, x_{33}, x_{41}
3	748 pb	z_{11} , z_{12} , z_{31} , z_{32} , z_{41}	s_{21} , s_{42}	x_{13}, x_{21}, x_{23}, x_{33}, x_{41}
4	748 pb	z_{11} , z_{12} , z_{31} , z_{32} , z_{42}	s_{22} , s_{41}	x_{13}, x_{21}, x_{23}, x_{33}, x_{41}

Tablo 10. R_eIMF ve SD − R_eIMF Model Sonuçlarının Değerlendirilmesi
(Evaluation of R_eIMF and SD − R_eIMF Models Results)

(Plan No) - H(z)		Yasaklama Sonrası Talep Noktalarının Hizmet Aldığı Tesisler x_{ij}	
R_eIMF	SD − R_eIMF	R_eIMF	SD − R_eIMF
(1) - 742	(1) - 748	x_{13}, x_{21}, x_{33}, x_{43}	x_{13}, x_{21}, x_{23}, x_{33}, x_{41}
(2) - 742	(2) - 748	x_{13}, x_{21}, x_{33}, x_{43}	x_{13}, x_{21}, x_{23}, x_{33}, x_{41}
(3) - 742	(3) - 748	x_{13}, x_{21}, x_{33}, x_{43}	x_{13}, x_{21}, x_{23}, x_{33}, x_{41}
(4) - 742	(4) - 748	x_{13}, x_{21}, x_{33}, x_{43}	x_{13}, x_{21}, x_{23}, x_{33}, x_{41}

iyi amaç fonksiyonu değeri olan 748 pb. elde edilmiştir. Tablo 10'da önerilen her iki modelinde, savunma planlayıcılarının aynı tesisleri koruduğu görülmektedir. Bununla birlikte yasaklama sonrası kapasite kısıtlı örnek için aynı talep noktasının farklı tesislerden hizmet aldığı görülmektedir. 2 numaralı talep noktası, kapasite kısıtı sebebi ile hem 1 no.lu, hem de 3 no.lu tesisten hizmet almaktadır.

5. SONUÇLAR (CONCLUSIONS)

Kritik tesislerin korunma planlaması, bir ülkenin savunması açısından öncelikli konulardandır. Bu çalışma kapsamında ele alınan bu problem iki seviyeli yasaklama/koruma modeli olarak ele alınmıştır. Çalışmada iki yeni matematiksel model önerilmiştir. İlk katkı olarak, önceki çalışmalarda göz ardı edilmiş olan farklı saldırı ve farklı savunma tipleri göz önüne alınmıştır. Ayrıca kaynak miktarının da sınırlı olabileceği ve saldırganın bu nedenle öncelikle arz-ve talep arasındaki dengeyi bozmayı hedefleyeceği bir matematiksel model (SD − R_eIMF) geliştirilmiştir. Bu modelde hizmet alan tesislerin tedarikinin tam karşılanamadığı durum göz önüne alınmıştır.

Saldırı ve savunma tiplerinin dahil edilmesi ve kapasite kısıtlarının göz önüne alınması ile modeller karmaşıklaşmış ve çözümleri güçleşmiştir. Modeller askeri ve kritik tesisler göz önüne alınarak tasarlanmıştır. Konunun hassasiyeti ve güvenlik konularında gerçek veriye ulaşma güçlüğü, test verisi türetmeyi gerektirmiştir. Örnek problemlerin çözümünde, modelin üst seviyesi için olası tüm alternatif savunma planları belirlenmiştir ve her bir savunma planına karşı saldırganın seviyesi için GAMS CPLEX çözücü ile en iyi saldırı planları belirlenmiştir. Bu saldırı planlarının en az maliyeti oluşturduğu koruma planları R_eIMF modelinin belirlediği eniyi koruma planlarıdır. Aynı şekilde SD − R_eIMF modeli de öncelikle arz-talep dengesinin bozulmasına neden olacak yasaklama tiplerine karşı koruma planlarını belirlemiş ve bunların içinden maliyeti en düşük olan koruma planlarını ve tesis - talep merkezi eşleştirmelerini belirlemiştir. Çalışmanın hem yerel güvenlik sistemlerinde ayrıca makro ve stratejik boyutta ülke güvenliğini tehdit edebilecek unsurlara karşı strateji geliştirme süreçlerinde yer bulabileceği görüşü motivasyon kaynağı olmuştur. Söz konusu tehditlerin sadece terörist eylemler, savaş vb. istenmeyen durumlarda ortaya çıkabilecek durumlar ile ilişkili olarak düşünülmemesi gerektiği, örneğin bir elektrik, doğalgaz, bilgisayar şebekesinde de rassal olarak karşılaşılabilecek bir arızanın da geliştirilen modellerde için bir çeşit tehdit olarak yer bulabileceği düşünülürse bu yaklaşımların kullanımının yaygın etkisi olabilecektir. Öte yandan büyük boyutlu problemlerin çözümünde ortaya çıkacak güçlük sebebiyle sezgisel yaklaşımlara ihtiyaç olabilecektir. Bu yönleriyle gelecek çalışmalara ışık tutabilmektedir.

KAYNAKLAR (REFERENCES)

1. Stackelberg H., The theory of market economy, Oxford: Oxford University Press, 1952.
2. Scaparra M.P., Church R.L., A bilevel mixed-integer program for critical infrastructure protection planning, Computers and Operations Research, 35, 1905-1923, 2008.
3. Wollmer R., Removing Arcs from a Network, Operations Research, 12 (6), 934-940, 1964.
4. Israeli, E., Wood, R. K., Shortest-path network interdiction, Networks 40 (2), 97–111, 2002.
5. Cappanera P., Scaparra M. P., Optimal allocation of protective resources in shortest-path networks, Transportation Science 45 (1), 64–80, 2011.
6. Shimizu K., Ishizuka Y., Bard J. F., Nondifferentiable and two-level mathematical programming, Springer Science & Business Media, 2012.
7. Wood R. K., Deterministic network interdiction, Mathematical and Computer Modelling 17 (2), 1–18, 1993.

8. Cormican K. J., Morton D. P., Wood R. K., Stochastic network interdiction, Operations Research 46 (2), 184–197, 1998.

9. McMasters A. W., Mustin T. M., Optimal interdiction of a supply network, Naval Research Logistics Quarterly 17 (3), 261–268, 1970.

10. Assimakopoulos N., A network interdiction model for hospital infection control, Computers in Biology and Medicine 17 (6), 413–422, 1987.

11. Farley J. D., Breaking al qaeda cells: A mathematical analysis of counterterrorism operations (a guide for risk assessment and decision making), Studies in Conflict & Terrorism 26 (6), 399–411, 2003.

12. Morton D. P., Pan F., Saeger K. J., Models for nuclear smuggling interdiction, IIE Transactions 39 (1), 3–14, 2007.

13. Washburn, A., Wood, K., Two-person zero-sum games for network interdiction, Operations research 43 (2), 243–251, 1995.

14. Xiang Y., Wei H., Joint optimizing network interdiction and emergency facility location in terrorist attacks, Computers & Industrial Engineering, 144, 106480, 2020.

15. Ramamoorthy P., Jayaswal S., Sinha A., Vidyarthi N., Hub Interdiction & Hub Protection problems: Model formulations & Exact Solution methods, Indian Institute of Management Ahmedabad India, 2016.

16. Aliakbarian N., Dehghania F., Salari M., A bi-level programming model for protection of hierarchical facilities under imminent attacks, Computers & Operations Research 64 210–224, 2015.

17. Church RL, Scaparra MP, Middleton RS, Identifying critical infrastructure: the median and covering facility interdiction problems, Ann Assoc Am Geogr, 94 (3) 491–502, 2004.

18. Salmeron J., Wood K., Baldick R., Analysis of Electric Grid Security Under Terrorist Threat, IEEE Transactions on Power Systems, 19, 2, 2004.

19. Salmeron J., Wood K., The Value of Recovery Transformers in Protecting an Electric Transmission Grid Against Attack, IEEE Transactions on Power Systems, 30, 5, 2015.

20. Aksen D., Aras D., A bilevel fixed charge location model for facilities under imminent attack, Computers & Operations Research, 39, 1364–1381, 2011.

21. Losada C., Scaparra M.P., Church R.L., On a bi-level formulation to protect uncapacitated p-median systems with facility recovery time and frequent disruptions, Electronic Notes in Discrete Mathematics 36, 591–598, 2010.

22. Losada C., Scaparra M.P., O'Hanley J.R., Optimizing system resilience: A facility protection model with recovery time, European Journal of Operational Research, 217, 519–530, 2012-a.

23. Aksen D., Aras A., Piyade N., A bilevel p-median model for the planning and protection of critical facilities, Journal Heuristics, 19, 373-398, 2013.

24. Lezama J.M.L., Gomez J.C., Galeano N. M., Assessment of the Electric Grid Interdiction Problem using a nonlinear modeling approach, Electric Power Systems Research, 144, 243–254, 2017.

25. Forghani A., Dehghanian F., Salari M., Ghiam Y., A bi-level model and solution methods for partial interdiction problem on capacitated hierarchical facilities, Computers and Operations Research, 114, 104831, 2020.

26. Wu X., Conejo A.J., An Efficient Tri-Level Optimization Model for Electric Grid Defense Planning, IEEE Transactions on Power Systems, 32, 4, 2017.

27. Alguacil N., Delgadillo A., Arroyo J.M., A trilevel programming approach for electric grid defense planning, Computers & Operations Research, 41, 282–290, 2014.

28. Jian G.J., Liu X., Sun L., Yin J., Optimal allocation of protective resources in urban rail transit networks against intentional attacks, Transportation Research Part E 84, 73–87, 2015.

29. Losada C., Scaparra M.P., Church R. L., Daskin M. S., The stochastic interdiction median problem with disruption intensity levels, Ann Oper Res, 201, 345–365, 2012.

30. Ghaffarinasaba N., Atayi R., An implicit enumeration algorithm for the hub interdiction median problem with fortification, European Journal of Operational Research, 267, 23–39, 2018.

31. Ramamoorthy P., Jayaswal S., Sinha A., Vidyarthi N., Multiple allocation hub interdiction and protection problems: Model formulations and solution approaches, European Journal of Operational Research, 1–16, 2018.

32. Xiao Y., Yang P., Zhang S., Zhou S., Chang W., Zhang Y., Dynamic Gaming Case of the R-Interdiction Median Problem with Fortification and an MILP-Based Solution Approach, Sustainability, 12, 581, 2020.

33. Salmeron J., Deception Tactics for Network Interdiction: A Multiobjective Approach, Networks an International Journal, 60, 45-58, 2012

34. Aksen D., Piyade N., Aras N., The budget constrained r-interdiction median problem with capacity expansion, CEJOR, 18, 269–291, 2010.

35. Keçici S., Aras N., Verter V., Facility network design under the threat of terrorist attacks, Springer Verlag, Optim Lett, 6, 1101–1121, 2012.

36. Zhu Y., Zheng Z., Zhang X., Cai K., The r-interdiction median problem with probabilistic protection and its solution algorithm, Computers & Operations Research 40, 451–462, 2013.

37. Liberatore F., Scaparra M.P., Daskin M.S., Analysis of facility protection strategies against an uncertain number of attacks: The stochastic r-interdiction median problem with fortification, Computers & Operations Research, 357–366, 2011.

38. Aksen D., Akca S.Ş., Aras N., A bilevel partial interdiction problem with capacitated facilities and demand outsourcing, Computers & Operations Research 41, 346–358, 2014.