# Oyun Teorisinin İnternet Ortamında Saldırı Tespit Sistemlerinde Kullanılması Üzerine Bir Araştırma

**Serap Ergün[1], Tuncay Aydoğan[2], Sırma Zeynep Alparslan Gök[3]**

[1] Süleyman Demirel Üniversitesi, Elektronik Haberleşme Mühendisliği Bölümü, Isparta

[2] Süleyman Demirel Üniversitesi, Yazılım Mühendisliği Bölümü, Isparta

[3] Süleyman Demirel Üniversitesi, Matematik Bölümü, Isparta

serapbakioglu@sdu.edu.tr, tuncayaydogan@sdu.edu.tr, sirmagok@sdu.edu.tr

**Özet:** Bilişim sistemleri güvenliği konusunda yapılan araştırmalar ve projeler internetin askeri, e-devlet, e-sağlık, e-ticaret, e-öğrenme, gibi konularda tüm dünyada yaygın olarak kullanılmaya başlamasıyla birlikte hız kazanmıştır. Günümüzde de bilişim sistemleri güvenliği alanındaki araştırmalar devam etmektedir. Bilgisayar ağlarında taşınan, işlenen ve saklanan bilgilerin artmış olması, güvenliğin dolayısıyla da güvenlik araştırmalarının önemini daha da artırmıştır. Bilişim sistemlerine bağımlılığımız gün geçtikçe arttığından, bu sistemlerin ve bunlar üzerinde işlenen, üretilen, saklanan ve iletilen bilginin güvenliğinin önemi de bağımlılığa paralel olarak artmaktadır. Bu çalışmada oyun teorisi bilişim güvenliği kavramlarından ve saldırı tespit sistemlerinden bahsedilmiştir. Bilgisayar ağlarında oyun teorisinin kullanılması araştırılmış ve geniş bir literatür özetine yer verilmiştir. Çalışmalarda genel olarak bilgisayar ağına saldıran ve bilgisayar ağını savunanlar arasında oyunlar modellenerek, oyuncuların seçmesi gereken stratejiler belirlenerek oyunun Nash dengesinin bulunması için çeşitli yöntemler geliştirilmiştir.
**Anahtar Sözcükler:** Oyun teorisi, Nash dengesi, strateji, bilişim güvenliği, saldırı tespit sistemleri

**Abstract:** Information systems security in research and projects web's military, e- government, e -health, e -commerce, e -learning, on topics such as common around the world as the beginning of the application have been accelerated. Today, in the field of information systems security research is ongoing. Computer network transported, processed, and stored information has increased the security of the thus increased the importance of security research. Our reliance on IT systems has increased day by day, and their processed on this system, manufactured, stored and transmitted the importance of information security is increasing in parallel with the addiction. In this study, game theory, IT security and intrusion detection systems of the concepts are discussed. The use of game theory in computer networks have been investigated and are included in an extensive literature summary. Working in the overall computer network attack and computer network games between defending modeled, players must choose their strategies for determining the existence of the Nash equilibrium of the game a variety of methods have been developed.

## 1. Giriş

1990'lı yıllarda yaşanan hızlı teknolojik gelişmelerin bir sonucu olarak bilgisayarlar, modern hayatın her alanına girmiş ve vazgeçilmez bir biçimde kullanılmaya başlanmıştır. Hayatımızın birçok alanında bilgisayar ve bilgisayar ağı teknolojileri "olmazsa olmaz" bir şekilde yer almaktadır. İletişim, para transferleri, kamu hizmetleri, askeri sistemler, elektronik bankacılık, savunma sistemleri, bu alanlardan sadece birkaçıdır. Teknolojideki bu gelişmeler, bilgisayar ağlarını ve sistemlerini, aynı zamanda, bir saldırı aracı haline, kullandığımız sistemleri de açık birer hedef haline getirmiştir.

Bilişim sistemlerine ve bu sistemler tarafından işlenen verilere yönelik güvenlik ihlalleri inanılmaz bir hızla artmaktadır. Bilişim sistemlerine olan bireysel ve toplumsal bağımlılığımız arttıkça bu sistemlerde meydana gelebilecek arıza ve saldırılara karşı duyarlılığımız da o denli artacaktır. Bu duyarlılık arttıkça da bilgisayar sistemlerine ve ağlarına yönelik olarak gerçekleştirilecek olan saldırıların sonucunda; para, zaman, prestij ve değerli bilgi kaybı da artacaktır. Bu saldırıların hastane bilişim sistemleri gibi doğrudan yaşamı etkileyen sistemlere yönelmesi durumunda ise kaybedilen insan hayatı bile olabilir.

Uygulamalı matematik alanında kullanılan oyun teorisinin ekonomi, sosyal bilimler gibi konularda kullanılırken son yıllarda bilgisayar ağlarında, bilişim/internet güvenliğinde ve kriptoloji gibi özel alanlarda da kullanıldığı yapılan çalışmalarda görülmektedir.

## 2. Oyun Teorisi

Oyun Teorisi, en genel ifadesiyle, akılcı bireylerin seçimleri ve bunların karşılıklı etkileşimlerinin sonuçlarını inceler. Bir oyunu tanımlayan en önemli unsur, oyuncuların sahip oldukları bilgidir. Bu teori oyun şeklinde ifade edilebilen her türlü durumu kapsar. Herhangi bir durumun oyun olarak değerlendirilebilmesi için ise şu üç koşulun birlikte sağlanmış olması gerekir [1]: Oyuncu olarak adlandıracağımız kişiler kümesi, her oyuncu için mümkün olan seçenekler kümesi, her bir seçeneğe ilişkin sonuçlar kümesi

Oyun Teorisi, ilk olarak 1920'li yıllarda matematikçi John Von Neumann [2] tarafından kâğıt oyunlarında en iyiyi oynamak amacıyla ortaya atılmıştır. Bu tür oyunlarda bazı oyuncuların kazançları diğerlerinin kaybı olduğundan toplam kazanç sıfır olur. Bu sebeple bu tür oyunlara sıfır toplamlı ikili oyunlar denmiştir. Askeri operasyonlar da bu oyunlar gibi düşünülebilir. Özellikle 1940' lı savaş yıllarında bu oyunlar son derece önem kazanmıştır.

Oynanmış ve günümüzde hala oynanmakta olan birçok oyunun kendisiyle ilişkilendirilmiş bir takım kuralları vardır. Bu oyunlara örnek olarak futbol, golf, basketbol tenis gibi oyunlar poker ve briç gibi kart oyunları ile satranç ve tavla gibi oyunlar verilebilir. Bütün bu oyunlar bir etkileşim bir rekabet unsuru içermektedir. Yani oyunda bir oyuncu diğer oyuncularla rekabet etmektedir ve oyuncunun başarısı, kendi hareketlerinin yanı sıra diğer oyuncuların hareketlerine de bağlıdır [3].

1950 yılında John Nash çözüm ve denge noktası olarak da bilinen ve günümüzde en çok kullanılan Nash dengesi teorisini oluşturmuştur [1].

### 2.1. Oyun Teorisi ile İlgili Kavramlar

Oyun teorisinin tanımına geri dönersek; "İki ya da daha fazla rakibi belirli kurallar altında birleştirerek karşılıklı olarak çelişen olasılıklar karşısında, birbirlerine karşı en doğru stratejiyi belirleme yöntemidir" şeklinde tanımlamıştık. Bu tanıma göre bir oyunda oyuncular, yunun kuralları ve stratejiler, oyunda elde edilen kazanç veya kayıplar (payoff), oyunun sonucu ya da denge noktası unsurlarının bulunması gerekmektedir.

a) Oyuncu: Bir oyunda her bir karar veren birime oyuncu denir ya da bir başka ifadeyle; oyunun taraflarına oyuncu denir. Bu oyuncular poker oyununda olduğu gibi bireyler, oligopol piyasalarda olduğu gibi firmalar veya askeri çatışmalarda olduğu gibi uluslar da olabilir [2]. Bir oyunu oynayabilmek için en az iki oyuncuya ihtiyaç vardır. Her oyuncu kendi bilgi seti ve rakibinin bilgi seti doğrultusunda faydasını maksimize edecek şekilde rasyonel olarak hareket ettikleri varsayımı altında hareket ederler. Rasyonel olmayan hareketlerin hiçbiri oyun teorisi içinde yer alamaz. Kısacası her oyuncu sahip olduğu tercihler arasında, mümkün olan en büyük ödülü verecek tercihi seçerek oyunu bitirmek arzusundadır.

b) Oyunun kuralları ve stratejiler: Bir oyunun oynana bilmesi için oyuna taraf olan oyuncuların belirli kurallar altında birleşmeleri gerekmektedir. Kuralların olmaması durumunda taraflar stratejilerini belirleyemeyeceklerdir. Bu kurallar satranç oyununda olduğu gibi her taşın nasıl hareket edeceği, şirketlerin ticaretini bir düzende tutan ticaret kanunu ya da uluslararası anlaşmalarla belirlenen kurallar olarak da ifade edilebilir. Stratejiler ise; her oyunda oyuncuların belli hareketler içerisinde çeşitli seçenekleri vardır. Oyuncuların belirli bir zaman dilimi içerisinde rakibinin olası hareketlerine karşı önceden belirlenen ve olanaklı alternatiflerden rakibin hareket tarzlarını saptayan kurallar bütününe strateji denir. Bir oyunda strateji sayısı sonlu ya da sonsuz olabilir [4]. Yapılan hareketin diğer oyuncuyu etkilemesi ve etkileşim sürecinin sürekli olması, o sürecin oyun olmasını sağlayacaktır.

c) Oyunda elde edilen kazanç ve kayıplar: Oyunun oynanması süresince her bir stratejiye karşılık gelen, her oyuncunun bir kazancı ya da bir kaybı söz konusudur. Bu kazanç ya da kayıplar artı sonsuz ile eksi sonsuz arasında yer alabilir. Bu değerler sayısal olarak ifade edilebileceği gibi, oransal olarak da ifade edilebilir. Kazançlar ya da kayıpların birimleri her durumda aynı ölçü biriminde olması gerekmektedir. Oyuncuların strateji seçimlerinden ortaya çıkan kazanç ve kayıpları göstermek için kullanılan matrise ise ödemeler matrisi adı verilmektedir.

d) Oyunun sonucu ya da denge noktası: Her oyuncunun rasyonel olarak hareket ettikleri varsayımı altında, oyuncuların oyunu bitirmeleri sonucunda ulaştıkları noktaya, oyunun sonu ya da denge noktası adı verilir. Oyun teoreminde bu denge noktasına Nash dengesi adı verilmektedir. Bu noktada her oyuncunun oynayacağı strateji belli olup, sözü edilen bu stratejiyi kullanmak için karar verilen hareketler uygulanır.

### 2.2. Denge Kavramı ve Nash Dengesi

Oyuncuların oyunu bitirmeleri sonucunda ulaştıkları noktaya, oyunun sonu ya da denge noktası adını vermiştik. Bu noktada, oyuncuların seçtikleri stratejiler $a= (a_i,a_{-i})$ şeklinde ifade edilir. Bu gösterimde yer alan $a_i$, i'inci oyun stratejisini verirken, $a_{-i}$ diğer oyuncunun stratejisini vermektedir.

Oyunun oynanması durumunda, her oyuncunun stratejisi olacaktır. Bu stratejiler içinde oyuncular kendi baskın stratejisinin olmasını arzularlar. Bu şekilde baskın stratejiye sahip olan oyuncular oyunun ne şekilde oynayacaklarını ve oyunun sonucunun ne şekilde biteceğini bilmek oldukça kolay hale gelmektedir. Baskın stratejiyle bir oyuncunun karşıdaki oyuncu ya da oyuncular ne şekilde oynarlarsa oynasınlar tek bir biçimde oyuncunun hareket etmesi anlamına gelmektedir.

Çoğu oyunların hâkim stratejileri yoktur ve oyuncular kendi hareketlerini seçmek için diğer oyuncunun hareketlerini ortaya çıkarmak zorundadır. Bu bakımdan oyuncular, diğer oyuncuların kararları veri iken yapabileceklerinin en iyisini yapacaklardır. Bu da hâkim strateji dengesini de içine alan ve daha geniş bir denge kavramı olan Nash dengesidir. Nash dengesi çok geniş oyunlar sınıfında çok kuvvetli tahminle üreten bir çözüm kavramıdır [1].

Nash dengesinde temel unsur, bir denge noktası düşüncesidir. Analizde Nash, von Neumann minimax teoremi genelleştirilmesinin temeli olarak en iyi cevap yaklaşımını seçmiştir. Nash' e göre, iki kişilik bir oyunun çözümüne aday olacak bir strateji çifti, stratejinin her biri rakibinin oynayacağını tahmin ettiği diğerine, en iyi cevap verebilme niteliğini sağlaması gerekmektedir. Bir denge noktası diğer oyuncuların stratejileri hususunda karar verdikleri inanılıyorsa, her bir oyuncunun stratejilerinin, oyuncunun kendi ödülünü maksimize ettiği durumu ifade etmektedir. Her bir oyuncunun stratejisi, diğer oyuncuların oynayacağını tahmin ettiği stratejilerine karşı optimaldir. Bu özellikleri olan bir strateji çifti (kombinasyonu) Nash dengesi olarak isimlendirilmekte, işbirliksiz oyunların temelini oluşturmaktadır [5].

Bu durumda oynanan herhangi bir durumda oyunda oyuncular için baskın stratejilerin bulunması sonucunda ulaşılan denge durumunun aynı zaman da Nash dengesine karşılık geldiğini söylemek mümkündür. Buna karşılık her Nash dengesi baskın stratejiye sahip ortaya çıkaran dengeyi vermek zorunda değildir. Çünkü kimi oyunlarda birden fazla Nash dengesine ulaşılması mümkündür [6].

### 2.3. Strateji Kavramı

Oyunlar teorisinin temel kavramlarından birisi strateji kavramıdır. Strateji kombine edilmiş kararlar dizisidir. Daha açık bir şekilde söylemek gerekirse Strateji, oyunun başından sonuna dek ortaya çıkabilecek bütün durumlar için oyuncuların tercihlerini belirten kararlar bütünüdür [1].

Oyunda tek bir denge noktası varsa hamle sayısı ne olursa olsun oyuncular bütün oyun boyunca tek bir strateji kullanacaklardır. Oyuncunun kullandığı bu tek stratejiye Salt Strateji denir. Bazı oyunlarda tek yerine birden fazla denge noktası vardır. Bu durumda oyuncular hamlelerinin bir kısmında bir oyun, diğer kısımlarında başka bir oyun uygulama imkânına sahiptirler. Böylece oyuncuların bir oyun süresince birden fazla hareket tarzını seçebilmelerine ve çeşitli kararları bir arada benimsemelerine Karma Strateji uygulaması denir.

Oyunlar teorisinin amacı rekabet etmekte olan, beklentileri zıt iki oyuncu için rasyonel hareket yollarını sezmektir. Tekrarı mümkün oyunlarda bir oyun için optimum strateji mümkün en büyük ortalama kazancı garanti edecek stratejidir. Rakip yönünden beklenen optimum strateji ise mümkün en küçük ortalama kaybı garanti edebilecek bir stratejidir.

### 2.4. Ödemeler (Getiri-Kazanç) Matrisi

Oyuncuların strateji seçimlerinin türlü bileşimlerinden sonuçlanan kazanç ve kayıpları gösteren matrise ödemeler matrisi denir. Ödeme matrisinin elemanları pozitif, negatif veya sıfıra eşit olabilir. Söz konusu matrisin herhangi bir elemanı pozitifse, sütunda yer alan oyuncu, satırda yer alan oyuncuya bu miktarda ödeme yapar. Matrisin herhangi bir elemanı negatif ise satırdaki oyuncu sütundaki oyuncuya bu negatif elemanın mutlak değerine eşit ödemede bulunur. Matrisin elemanı sıfır ise oyunculardan hiçbiri birbirine ödemede bulunmaz.

## 3. Saldırı Tespit Sistemleri

Saldırı Tespit Sistemleri (Intrusion Detection System – IDS - STS), bilgisayarların ve bilgisayar ağlarının faaliyetlerini izlemek, kaydetmek ve olası saldırıları tespit etmek amaçlı olarak tasarlanan sistemlerdir.

Anderson yayınladığı raporunda [7] saldırıyı, "izinsiz olarak bilgiye ulaşmak, değiştirmek, sistemi kullanılmaz veya güvenilmez hale getirmektir" diye tanımlamaktadır. İnternet ve bilgisayar teknolojilerindeki gelişmeleri göz önünde bulundurarak yeni bir tanım yapabiliriz. Anderson'un yaptığı bu tanımı genişletirsek bilginin gizliliği, bütünlüğü ve erişilebilirliğinin bozulması yönünde yapılan her türlü girişime saldırı demek mümkündür.

Veri gizliliği verinin yetkisiz birine karşı veya üçüncü şahıslara ifşasını engeller. Veri bütünlüğü verinin doğruluğu, aslına uygun ve bozulmadığı ile ilgilenir. Erişilebilirliğinin bozulması ise hizmetin önceden belirlenmiş bir hizmet kalitesinin altına düşmesi veya verilen hizmetin tamamen işlemez veya erişilemez hale gelmesi anlamını taşımaktır. Sistem için hizmet aksatma büyük bir tehdittir [8].

Saldırı tespiti ise ağ üzerinde akan verinin üçüncü şahıs veya sistemler ile izlenerek gizliliğinin, bütünlüğünün ve erişilebilirliğinin kısmen veya tamamen bozulması halinin tespit edilmesidir.

Bilgisayar ağlarında yapılan her türlü yetkisiz erişimin tespit edilmesi ve ağ içerisinde oluşan anormalliklerin gözlenmesi, akan trafiğin analizi ile mümkün olmaktadır. STS'ler ağ ve ağdaki bilgisayarların çalışmalarını izleyerek veri toplar. Toplanan veriler önceden tespit edilen saldırı motiflerine veya saldırı imzalarının yer aldığı veri tabanları ile karşılaştırılarak analiz edilirler. Analiz sonucunda kötü niyetli bir girişim tespit edilir ise STS'ler bir mesaj veya bir alarm oluşturarak ağ yöneticilerini uyarırlar.

## 4. Önceki Çalışmalar

Furuncu ve Soğukpınar [9] bulut bilişim kullanılması durumunda ideal güvenlik önlemlerinin bulunmasında yardım etmektedir. Çünkü günümüz yöntemleri bulut bilişimde saldırgan ve savunanın kazançlarını ve masraflarını ön plana çıkarmamaktadır. Önerilen modelde ekonomide çok sık kullanılan oyun teorisini kullanarak saldırgan ve savunanın çıkar modellemesi yapılmıştır. Savunanın ideal güvenlik stratejisi sunucu değerlerine ve sunucu üstündeki saldırı risklerine bakılarak hesaplanmıştır. Bu model, sabit olarak sadece bulut bilişimdeki objelerin birbirleri ilişkilerine bakarak, aralarında oluşabilecek riskleri bulut bilişimin altyapısını oluşturan devasa kod üzerinde aramaktan daha hızlı verimli olmaktadır.

Gueye vd. [10], bir ağın topolojisi verilerek adressiz (yönsüz) bir grafik ile karakterizasyonu yapılarak şu oyun durumu üzerinde çalışılmışlardır: Bir ağ yöneticisi grafiği kapsayan bir ağaç (iletişim altyapısı gibi) seçmektedir ve saldırgan iletişim ağacını ağın tek bir kolu üzerinden bozmaya çalışıyor. Saldırganın saldırma maliyeti olduğu gibi ağa hiç saldırmama seçeneği de vardır. Ağ yöneticisi ve saldırgan arasındaki etkileşim bimatrix oyun olarak modellenmiş ve Nash dengelerinden oluşan kümeler ile çalışılmıştır. Saldırı maliyetinin olduğu durumlarda, bağlantıların önemli bir alt kümesi kavramı tanımlanmış ve Nash dengelerinden oluşan bir dizini yapısı belirlenmiştir. Bu yapıda, saldırgan kritik altkümelerde hedef belirler ve aynı kritik altküme aynı olasılıkla saldırıya uğrar. Sıfır maliyetli saldırılar için ise, Nash dengelerinden oluşan küme karakterize edilmiştir.

Gueye ve Walrand [11] çalışmalarında, ağa saldıran ve ağı savunan (ağ kullanıcısı) arasında modellenen oyunda ağ güvenliğini araştırmışlardır. Oyunda, saldırgan ve savunan birbirlerinin en iyi stratejilerini tahmin etmeye çalışır. Saldırıya karşı en iyi savunmasını hesaplanan Nash dengesi sayesinde belirler. Çalışmada, iki çeşit problem üzerinde durulmuştur. Birinci tip problem, verilerin saldırgan tarafından değiştirilebildiği ağlardır. Böyle bir saldırının var olma ihtimali göz önüne alındığında, ağ kullanıcısı gözlemlediği veriye güvenip güvenmeyeceğine karar verirken saldıran verileri nasıl bozacağına karar verir. Ağ kullanıcısının küçük bir maliyetle iletilerin geçerliliğini test etme imkânı varsa, bu maliyetle saldıranı cezalandıracağını belirtir. Böylece ağı güvenilir yapmak için saldırı olasılığını azaltmış olur. İkinci tip problem, virüs saldırılarıdır. Virüs yazılımcısı virüsün ne kadar agresif olacağına karar verirken, savunan virüs tespiti için bir mekanizma seçer. Virüs çok agresif olduğunda, tespit etmesi kolay olduğundan virüsün

agresifliğinde optimum bir seviye belirlenmeye çalışılır. Böylece sistem, virüsün agresifliğini sınırlama konusunda virüs tasarımcısını zorlar.

Kodialam ve Lakshman [12] çalışmalarında, bir iletişim ağında izinsiz bir paketin tespit edilmesi üzerinde çalışmışlardır. Algılama sistemi, ağ bağlantıları (veya yönlendirici arabirimleri) ile belirlenen transit paketlerin bir kısmının örneklenerek gerçekleştirilir. Gerçek zamanlı paket örnekleme için ağ maliyetlerinin üstlenilmediğinden, verilen toplam örnekleme bütçesini aşmadan etkin ağ saldırılarını tespit etmek için bir ağ paket örnekleme stratejisi geliştirilmiştir. Oyun teorisi çerçevesinde sorun ele alınarak, saldırganın seçtiği yolları (ya da sadece kısa yol yönlendirme mümkün olup olmadığını ağ giriş noktası) algılama olasılığı en aza indirilmiş ve şebeke operatörünün örnekleme stratejisi için seçmiş olduğu yolları algılama şansı en üst düzeye çıkarmışlardır. Problemi oyun teorisiyle formülüze ederek, optimal örnekleme planlarını geliştirmişlerdir.

Alpcan ve Tamer [13], ağ saldırılarının algılanarak bir karar verilmesi, analiz yapılması konusuna oyun teorisiyle bir yaklaşım getirmişlerdir. Hasic-dengeler, bilgi güvenliği ile ilgili analiz ve karar süreçleri, saldırı tespitlerinin yanı sıra oyun teorisi kavramlarının olası uygulamaları resmi bir karar ve denetim çerçevesi geliştirmek için araştırılmıştır. Dağıtık bir saldırı tespit sisteminin sensör bir ağ olarak kabul edilen genel modeli düşünülerek oyun teorisi tekniklerine dayalı iki şema önerilmiştir. Güvenlik uyarı sistemi basit ve uygulanması kolaydır. Sistem yöneticilerine ağ güvenlik durumuyla ilgili bilgi verir. Geliştirilen güvenlik saldırı oyunu; iki kişilik sıfır toplamlı olmayan, işbirliksiz dinamik bir oyun olarak modellenerek Nash dengeleri çözüm olarak sunulmuştur.

Siber saldırıların; internet sistemlerini sayı, kapsam ve zarar bakımından kötü olarak etkilemeleri arttıkça gerek akademik araştırmacıların gerekse sanayi uygulayıcılarının problemleri çözmeleri zorlu hale gelmiştir. Vu vd.[14], çalışmalarında siber güvenlik problemlerinde oyun teorisi yaklaşımlarının uygulanabilirliğini araştırarak, etkin bant genişliğini tüketen saldırılar üzerine odaklanmışlardır. Saldırgan ve savunan arasındaki etkileşimi iki kişili sıfır toplamlı olmayan oyun olarak iki senaryo dâhilinde modellemişler. Hizmet engelleme servisi (DoS) için tek bir saldırı ve dağıtık hizmet engelleme servisi (DDoS) için çoklu saldırı senaryolarını kullanmışlardır. Yapılan analizde, en kötü durum senaryosu dikkate alınarak saldırgan girişimleri nerede ise en etkili gönderme hızı veya botnet (saldırı yazılımı) boyutu belirlenir. Her iki durumda da savunan sistemin en iyi stratejisini temsil eden Nash dengesini hesaplamak için hem statik hem de dinamik oyunlar oluşturmuşlardır. Çalışmanın simülasyon kısmında NS-3 simülatörü kullanılarak, geniş simülasyon tabanlı deneyler yoluyla oyun teorisi yaklaşımının etkinliğini vurgulamışlardır.

Yeni fırsatlar sunan bilgi teknolojisi ve altyapısında önemli gelişmeler varken siber hala tamamen güvenli olmaktan oldukça uzaktadır. Birçok durumda kullanılan güvenlik çözümleri geçicidir ve aynı zamanda sayısal çerçevede karar vermeden yoksundur. Bu probleme çözüm olarak, sağlam bir analitik ortama dayalı bir savunma mimarisi oluşturmak için oyun teorisi büyük bir potansiyel olarak görülmektedir. Bedi vd. [15] çalışmalarında siber güvenlik sorunlarına oyun teorisi yaklaşımlarının uygulanabilirliğini araştırmışlar ve TCP/TCP üzerindeki etkin bant genişliği tükenmesi problemine odaklanmışlardır. Kullandıkları senaryolar ise Vu vd.' nin yapmış oldukları çalışmadaki [14] gibidir.

Jiang vd. [16] çalışmalarında, bilgisayar ağlarında saldırı tahminini ve aktif savunmayı analiz etmek için stokastik oyun teorisi yaklaşımı sunmuşlardır. Saldırgan ve savunan arasındaki etkileşimi baz alarak iki oyunculu, işbirlikçi olmayan sıfır toplamlı, sonlu stokastik oyun olarak formüle etmişlerdir. Saldırı stratejileri tahmini ve optimum aktif savunma stratejisi karar algoritması ADSG

(Attack-Defence Stochastic Game) ve maliyet-hassasiyet modeli ile geliştirilmiştir. Saldırıyı savunmak ve ağı önceden koruma altına almak için maliyeti en aza indirerek optimum savunma stratejileri kullanılmıştır. Son olarak, bir ağa karşı bir saldırı basit bir örnek üzerinde modellenerek analiz edilmiştir.

Cao vd. [17] çalışmalarında lider-takipçi, işbirlikçi ve iki kişili sıfır toplamlı olmayan oyunları yeniden yorumlayarak internet fiyatlandırma durumuna uygulamışlardır. İnternet hizmet kalitesi (QoS) için basit bir model ile, lider-takipçi oyununun Pareto optimum olmayan bir çözüm olabileceğini ve bazı durumlarda 'haksız' olabileceğini göstermişlerdir. Bu işbirlikçi oyun hem kullanıcı hem de internet servis sağlayıcısı (ISS) için daha iyi bir çözüm olabileceğini sunmuşlardır. Sonuçların pratik uygulamalardaki yeri hükümet düzenlemelerinde veya tahkimde yararlı olabilir olmasıdır. QoS modeli aynı zamanda iki servis sağlayıcı arasındaki rekabeti incelemek için kullanılır ve çalışmada işbirliği olmadan hareket edemeyen servis sağlayıcıları arasında bir Nash denge noktası bulmuşlardır.

## 5. Sonuç ve Öneriler

Bilişim sistemleri güvenliği konusunda yapılan araştırmalar ve projeler internetin askeri, e-devlet, e-sağlık, e-ticaret, e-öğrenme, gibi konularda tüm dünyada yaygın olarak kullanılmaya başlamasıyla birlikte hız kazanmıştır. Günümüzde de bilişim sistemleri güvenliği alanındaki araştırmalar devam etmektedir. Bilgisayar ağlarında taşınan, işlenen ve saklanan bilgilerin artmış olması, güvenliğin dolayısıyla da güvenlik araştırmalarının önemini daha da artırmıştır.

Bilgisayar ağlarında gizlilik, bütünlük ve sürekliliğin sağlanması için hali hazırda geliştirilmiş bilişim teknolojileri projeleri yanında son yıllarda iç tehdit, kişisel gizlilik, güvenli yazılım geliştirme, web uygulaması güvenliği, kablosuz mobil sensör ağları, RFID güvenliği, siber ataklar ve endüstriyel sistemler BT güvenliği konularında yeni projeler geliştirilmektedir. Bilişim sistemleri güvenliği alanında yeni çözümlerin geliştirilmesi daha güvenli bir iletişim ortamı sağlanmasına ve geliştiren kurum veya ülkenin teknoloji pazarında ön plana çıkmasını sağlayacaktır.

Bilişim sistemlerine bağımlılığımız gün geçtikçe arttığından, bu sistemlerin ve bunlar üzerinde işlenen, üretilen, saklanan ve iletilen bilginin güvenliğinin önemi de bağımlılığa paralel olarak artmaktadır. Bilişim sistemlerinin ve bu sistemler tarafından işlenen bilgilerin güvenliğinin sağlanması için yeni teknoloji yöntemlerinin kullanılmasında ve performanslarının analiz edilmesinde fayda vardır.

Oyun teorisinin güçlü bir algoritmik yapısı olduğundan, bilgisayar bilimine ait birçok problemin modellenmesinde kullanıldığı literatürdeki çalışmalarda Oyun teorisinin haberleşme ağlarına uygulanabilirliği, veri ağları üzerinde uygulamasını yapılabilirliği, ortam erişim, ağ güvenliği, güç kontrolü ve spektrum konusunda kullanılabilirliği görülmüştür.

İnternet ortamında güvenliğin ön planda olduğu saldırı tespit sistemlerinde saldırı-savunma temelinde oyunlar kurularak gerek işbirlikçi yaklaşımla gerekse işbirliği olmayan durumlarda modellemeler yapılarak sistemlerin performansları test edilmiştir. Literatür çalışmaları; oyun teorisi yaklaşımının rekabet içeren bilişim konularında başarılı sonuçlar vererek sistem güvenilirliğini, kullanıcı memnuniyetini sağlayarak zamandan tasarruf sağladığını göstermiştir.

## Kaynaklar

[1] Nash, J., F., 'Noncooperative Games. Annals of Mathematics', 1951, vol.54, s.289-295.

[2] Von Neumann, J., O. Morgenstern, 'Theory of Games and Economic Behaviour', 1944, Princeton University.

[3] Morton, D., 'Game Theory: A Nontechnical Introduction Paperback', 1997, Dover Publications.

[4] Özdil, T., 'Ekonomik Problemlerin Çözümünde Oyun Kuramının Yeri: Finansal Piyasalarda Bir Uygulama', 1998, Dokuz Eylül Üniversitesi, Sosyal Bilimler Enstitüsü, İktisat Anabilim Dalı, Doktora Tezi, İzmir.

[5] Çağlar, M., 'Oligopollistik Piyasalarda Karar Alma Süreçleri ve Oyun Teorisi', 2002, Gazi Üniversitesi, Sosyal Bilimler Enstitüsü, Doktora Tezi, Ankara.

[6] Kafadar, T., 'Stratejik Dış Ticaret Politikaları ve Teknoloji Transferi', 2002, İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Y.Lisans Tezi.

[7] Anderson, J., P., 'Computer security threat monitoring and surveillance. Technical Report',1980,Fort Washington, Pennsylvania, pp. 5-8, Washington.

[8] Vesely, A., Breclerova, D., 'Neural Networks in Intrusion Detection Systems', 2004, Agriculture Economy, 50, 2004 (1), pp. 35-39. Prague, Czech Republic.

[9] Furuncu, E., Soğukpınar, İ., ' Oyun Teorisi Kullanılarak Bulut Bilişimde Ölçeklendirebilir Güvenlik Değerlendirmesi', 2012, V. International Information Security and Cryptology Conference, pp.285-290, ISCTURKEY 2012, Ankara.

[10] Gueye, A., Walrand, J., C., Anantharam, V., 'A Network Topology Design Game: How to Choose Communication Links in an Adversarial Environment?.' , 2012, Game Theory for Networks Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering Volume 75, 233-248.

[11] Gueye, A, Walrand, J., C., ' Security in Networks: A Game-Theoretic Approach', 2008, Proceedings of the 47th IEEE Conference on Decision and Control Cancun, Mexico, Dec. 9-11.

[12] Kodialam, M., Lakshman, T., V., ' Detecting network intrusions via sampling: a game theoretic approach', 2003, Twenty-Second Annual Joint Conference of the IEEE Computer and Communications, IEEE Societies, Vol. 3. IEEE.

[13] Alpcan, T., Tamer B., ' A game theoretic approach to decision and analysis in network intrusion detection', 2003, Decision and Control, Proceedings, 42nd IEEE Conference on. Vol. 3. IEEE.

[14] Wu, Q., Shiva, S., Roy, S., Ellis, C., & Datla, V. 'On modeling and simulation of game theory-based defense mechanisms against DoS and DDoS attacks', 2010, In Proceedings of the 2010 spring simulation multiconference (p. 159). Society for Computer Simulation International.

[15] Bedi, H. S., Roy, S., & Shiva, S., 'Game theory-based defense mechanisms against DDoS attacks on TCP/TCP-friendly flows', 2011, InComputational Intelligence in Cyber Security (CICS), 2011 IEEE Symposium on(pp. 129-136). IEEE.

[16] Jiang, W., Tian, Z. H., Zhang, H. L., & Song, X. F., 'A stochastic game theoretic approach to attack prediction and optimal active defense strategy decision', 2008 In Networking, Sensing and Control, 2008. ICNSC 2008. IEEE International Conference on (pp. 648-653). IEEE.

[17] Cao, X. R., Shen, H. X., Milito, R., & Wirth, P., 'Internet pricing with a game theoretical approach: concepts and examples', 2002, Networking, IEEE/ACM Transactions on, 10(2), 208-216.