T.C.

FIRAT ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

# KABLOSUZ AĞLARDA YAPAY BAĞIŞIKLIK SİSTEMİ KULLANILARAK SALDIRI TESPİTİ VE GÜVENLİK

Erhan AKBAL

Tez Yöneticisi:
Yrd. Doç. Dr. Burhan ERGEN

YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

ELAZIĞ, 2007

T.C.

FIRAT ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

# KABLOSUZ AĞLARDA YAPAY BAĞIŞIKLIK SİSTEMİ KULLANILARAK SALDIRI TESPİTİ VE GÜVENLİK

Erhan AKBAL

Yüksek Lisans Tezi

Bilgisayar Mühendisliği Anabilim Dalı

Bu tez, ..... tarihinde aşağıda belirtilen jüri tarafından oybirliği /oyçokluğu ile başarılı / başarısız olarak değerlendirilmiştir.

Danışman: Yrd. Doç. Dr. Burhan ERGEN

Üye: Yrd. Doç. Dr. Ali KARCI

Üye: Yrd. Doç. Dr. Arif GÜLTEN

Bu tezin kabulü, Fen Bilimleri Enstitüsü Yönetim Kurulu'nun ...../...../..... tarih ve ..... sayılı kararıyla onaylanmıştır.

**TEŞEKKÜR**

Bu tez çalışmam boyunca, eski danışmanım Sayın Yrd. Doç. Dr. Ahmet ÇINAR' a ve ilgi ve yardımlarını esirgemeyen, çalışmalarımın oluşturulmasını ve tamamlanmasını sağlayan danışmanım Sayın Yrd. Doç. Dr. Burhan ERGEN' e, ayrıca çalışmam boyunca beni destekleyen ve yardımını esirgemeyen eşim, ailem ve tüm arkadaşlarıma sonsuz teşekkürlerimi sunarım.

# İÇİNDEKİLER

# ŞEKİLLER LİSTESİ

## TABLOLAR LİSTESİ

## KISALTMALAR LİSTESİ

Ab :Antikor
Aff :Duyarlılıklar
Ag :Antijen
AP :Erişim Noktası (Access Point)
ASH :Antijen Sunan Hücreler
AIS :Yapay Bağışıklık Sistemi (Artificial Immune System)
CTL :Sitotoksik T- Lenfositleri (Cytotoxic T Lenfosit)
DSL :Dijital Abone Hattı (Digital Subscriber Line)
IEEE :Elektrik Elektronik Müh. Enstitüsü (Institute of Electrical and Electronics Engineering)
Ig :İmmunoglobin
HIS :İnsan Bağışıklık Sistemi (Human Immune System)
LAN :Yerel Alan Ağı (Local Area Network)
LPT :Uzun İşlem Zamanları (Longest Processing Times)
MAN :Büyük Şehir Alan Ağı (Metropolitan Area Network)
Mbps :Saniye Başı Mega Bit (Mega Bit Per Second)
MHC :Ana Uyumluluk Karmaşığı (Major Histocompatibility Complex)
NK :Doğal Öldürücüler (Natural Killer)
NIC :Ağ Ara yüz Kartı (Network Interface Card)
Non-Self :Tanınmayan
PC :Kişisel Bilgisayar (Personal Computer)
PCI :Yan Bileşen Bağlantısı (Peripheral Component Interconnect)
PDA1 :Cep Bilgisayarı (Personal Digital Assistant)
RLAN :Radyo Yerel Alan Ağı (Radio Local Area Network)
RF :Radyo Frekansı (Radio Frequency)
Self :Tanınan
STS :Saldırı Tespit Sistemi
TCP :İletim Kontrol Protokolü (Transmission Control Protocol)
TCR :T hücre Reseptörü (T Cell Receptor)
WLAN :Kablosuz Yerel Alan Ağı (Wireless Local Area Network)
Wi-Fi :Kablosuz Sadakat (Wireless Fidelity)
VLAN :Sanal Lokal Alan Ağı (Virtual Local Area Network)
YBS :Yapay Bağışıklık Sistemi

# ÖZET

Yüksek Lisans Tezi

## KABLOSUZ AĞLARDA YAPAY BAĞIŞIKLIK SİSTEMİ KULLANILARAK SALDIRI TESPİTİ VE GÜVENLİK

**Erhan AKBAL**

Fırat Üniversitesi

Fen Bilimleri Enstitüsü

Bilgisayar Mühendisliği Anabilim Dalı

**2007, Sayfa: 75**

Kablosuz ağ sistemlerinin hızla çoğalması ve mobil uygulamaların gelişmesi ağ güvenliğini tehdit edecek unsurların artmasına neden olmuştur. Ağı korumak için kullanılan güvenlik duvarları, virüs yazılımları ve koruyucu programlar uzun süre sistemi korumakta yeterli olmamaktadır. İstenmeyen durumların sürekli artması ve bunlara karşı alınacak önlemlerde gecikilmektedir. Yapay bağışıklık sistemi (YBS) yardımıyla, herhangi bir müdahaleye gerek duymadan gecikmeksizin istenmeyen durumları tespit edilebilir. Böylece kablosuz ağ ve cihazlarını uzun süreli ve müdahalesiz korumak da mümkün olacaktır. Özellikle kablosuz ağlar, belirli bir noktaya bir fiziksel bağlantı olmadığı için saldırılara daha açık ve daha fazla koruma gerektirirler. Bu nedenle kablosuz ağlarda saldırı tespiti ve korunması daha zordur. Sunulan çalışmada, kablosuz ağlar üzerinde gerçekleştirilen model ile YBS uygulama sonuçları verilmiştir. Ağ cihazlarının uzun süre açık olması ve saldırıların bu uzun süre içerisinde olabileceği dikkate alınarak yeterli uzun sürede erişim noktası tabanlı YBS uygulaması gerçekleştirilmiştir.

Sonuç olarak oluşturulan yapı ile kablosuz alan ağlarında saldırı tespiti yapılmış ve yapay bağışıklık sisteminin çeşitli tasarım kriterleri değiştirilerek sistemdeki doğru tespit oranlarında değişik sonuçlar elde edilmiştir.

**Anahtar Kelimler:** Yapay Bağışıklık Sistemleri, Kablosuz Alan Ağları, Saldırı Tespit sistemleri

# ABSTRACT

My Thesis

## INTRUSION DETECTION AND SECURITY BY USING OF ARTIFICIAL IMMUNE SYSTEM AT WIRELESS NETWORKS

Firat University
Graduate School of Natural and Applied Sciences
Department of Computer Engineering

**2007, Page: 75**

The development of mobile application and rapidly increase of wireless system have arisen the number of elements threatening the security of network. The firewalls, anti-virus software and other security software to protect the network are insufficient in long term time. The anomalies have been rising and it could be too late to take precautions. It can be determined intrusion without any delay by means of Artificial Immune System (AIS). Thus, it can be possible to protect wireless networks and its equipment in long term time without any interference. Especially in wireless network, it is required more protection because there is no physically connection and it is defenseless for intrusions. In presented study, it is given the results of AIS application realized on wireless network for two approaches. The AIS application has been realized user node and access point based by taking into consideration that the network devices is works for long time periods and the intrusions may happen in this periods.

Finally, intrusion detections were realized in wireless network by an AIS structure, and it is observed the right detection rates while changing the various design criteria in AIS.

**Keywords:** Artificial Immune Systems, Wireless Local Area Network, Intrusion Detection Systems

# 1. GİRİŞ

İnsanoğlu çok eskilerden beri gerek doğada gerçekleşen olayları anlamak, gerekse bu işleyişleri adapte ederek yaşamını kolaylaştırmak üzere çoğu problemin çözümünü doğada aramıştır. Teknolojinin ilerlemesi, beraberinde çözümü karmaşık problemleri getirmiş ve bilinen yöntemler, karmaşıklaşan bu problemlerin çözümünde yetersiz kalmaya başlayınca, farklı çözüm yolları araştırılmaya başlanmıştır. Bunu takiben ortaya çıkan Yapay Sistemler, özellikle 1900'lü yılların ortalarından itibaren adını sıkça duyurmaya başlamıştır [1]. Bununla birlikte ağ iletişiminin gelişmesi ile internet modern bilim için önemli altyapılar üretmeye başlamıştır. İnternet kullanıcılarının hızlı artışı online tabanlı servislerin, kablosuz ve kablolu ağ uygulamalarının artmasına sebep olmuştur. Kablosuz ağlar kablolu ağlara göre daha fazla tehlikeye maruz kalabilmektedir. Bunun sebebi sinyalin hava üzerinden iletilmesidir. Ağ kullanıcılarının ve uygulamalarının artması kötü niyetli kişileri buraya yöneltmiştir. Bu sebeple çeşitli saldırı tespit sistemleri geliştirilerek ağların korunması amaçlanmıştır.

Saldırı Tespit Sistemleri (STS) oluşturulmasında çeşitli yaklaşımlar bulunmaktadır. Bu yaklaşımların temeli iki tekniği ortaya çıkarmıştır. Bunlar anormal durumları tespiti ve kötüye kullanımı engellemedir. Anormal durum tespiti yaklaşımı kullanıcıların, sistemlerin ve sistem kaynaklarının normal davranışlarının belirli profillerini çıkarılmasıyla, ağın tarayıcı programlarla bunların ayırt edilmesini temel almaktadır. Bu yaklaşım normal davranış profillerinden çeşitli tanımlamalarla saldırıların tespit edilmesidir. Kötüye kullanımı engelleme yaklaşımı bilinen sistem açıklarının ve tehlikeye maruz kalabilecek durumların belirlenerek bunların şüpheli kullanım olarak belirlenmesi yaklaşımına dayanır.

Çalışmada seçtiğimiz yaklaşım anormal durum tespitidir. Çünkü bu yaklaşım ile sadece bilinen saldırılar değil aynı zamanda bilinmeyen saldırıların tespitini de gerçekleştirme yeteneğine sahiptir. Çünkü YBS ile normal ağ davranışları başlangıçta tanımlanmakta ve sonrasında bu davranışların dışında gelebilecek herhangi bir anormal ağ davranışını tespit edebilmektedir. Çalışmada ağ üzerindeki paketlerden tanınanlar ile tanınmayan durumların ayrıt edilmesi sağlanmıştır. Böylece kablosuz alan ağlarında oluşabilecek güvenlik tehditlerini, yapay bağışıklık sistemi kullanılarak ne kadar etkin ve doğru bir şekilde tespit edilebileceği sonuçları ortaya konulmuştur. YBS' den kaynaklanan çeşitli sınırlamalar ile maksimum doğru tespit oranlarını, minimum performans kayıplarıyla tespit edilmesi gerekmektedir.

## 1.1. Tez Konusunun Tanıtılması

Tanıma, hafıza oluşumu, dağıtılmış mekanizma, hata toleransı gibi daha bir çok özelliği bünyesinde barındıran Bağışıklık Sistemleri, Yapay Zeka uygulamalarına elverişli bir model zemini oluşturarak Yapay Bağışıklık Sistemlerine temel hazırlamıştır. Bağışıklık sistemindeki pek çok özelliğin modellenmesi, birçok farklı alanda yeni YBS algoritmalarının oluşturulmasına vesile olmuştur.

İnsan bağışıklık sisteminin çalışma prensiplerinden esinlenilerek ortaya çıkmış olan yapay bağışıklık sistemleri, doğal bağışıklık sisteminin kullanmış olduğu mekanizmaları içermektedir. İnsan bağışıklık sisteminin en önemli özelliği vücudun normal davranışları ile normal olmayan davranışlarını ayırt etmektir. Çalışmada doğal bağışıklık sisteminin bu özelliği kullanılarak kablosuz alan ağlarında oluşabilecek tehlikeli durumları tespit etmek ve ağı bu durumlara karşı korumak amaçlanmıştır.

Çalışmada günümüzde oldukça fazla kullanılmaya başlanan ve geleceğin en önemli teknolojilerinden olan kablosuz alan ağlarında, oluşabilecek güvenlik sorunlarına, yapay bağışıklık sistemi algoritmalarını kullanarak önlemler almaktır. Kablolu ağlar ile kablosuz ağlar arasındaki farklar ortaya konularak kablolu ağlarda alınan güvenlik önlemlerinin kablosuz ağlara uygulanabilirliği araştırılmıştır.

## 1.2. Tezin Amacı ve Önemi

Son yıllarda hem kablolu ağlarda hem de kablosuz ağlarda güvenlik önemli bir konu olarak ortaya çıkmaktadır. Bu gibi sistemleri kullanan kurum ya da şirketler için en önemli konu bilginin güvenilirliği ve sistem üzerindeki kullanıcıların saldırılardan zarar görmemesidir. Ağ üzerindeki bilginin bir şekilde bozulması ya da başka kişilerin eline geçmesi yada ağ üzerindeki cihazların zarar görmesi kurum yada şirketleri maddi ve manevi olarak büyük kayıplara uğratabilmektedir.

Bu tezin amacı, kablosuz bir yerel alan ağında güvenlik unsurlarının neler olduğunu saptamak ve günümüzde popüler olan kablosuz ağlarda oluşan güvenlik açıklarına karşı önlem almaktır. Kablosuz bir ağa yapılabilecek herhangi bir saldırıda ne gibi önlemler alınabileceği konuları ortaya konmuştur. Böyle bir saldırıya karşı koymak içinde YBS kullanılmış ve bu sistemin nasıl çalıştığı insan bağışıklık sisteminin bir modeli çıkartılarak bir kablosuz ağda saldırı tespiti için kullanılabileceği ortaya konmuştur. Yapay bağışıklık sistemleri, doğal bağışıklık sisteminden esinlenerek, doğal sistemin prensiplerinin mühendislik açısından incelenerek karmaşık problemlerin çözümünde ve sistemlerin gelişiminde kullanılan sezgisel yöntemlerden biridir [1]. Çalışmada mevcut YBS uygulamalarından farklı olarak tespit işlemi için erişim noktası tabanlı bir model önerilmiştir. Bu model ile daha doğru ve etkin sonuçlar

elde etmek hedeflenmiştir. Buradaki amaç doğru tespit oranları elde etmekle beraber, dağıtıklık, kendi kendine organizasyon ve düşük maliyetler ile tespitin gerçekleştirilmesini sağlamaktır. Çalışmanın en önemli farkı düşük maliyetler getirmesidir. Düşük maliyet olarak ağ ve ağ cihazlarının performans kayıplarını minimuma indirmek amaçlanmıştır. Ayrıca mevcut STS yazılımlarından farklı olarak YBS ile kendi kendine organize olan ve tespit için herhangi ek bir müdahaleye gerek kalmadan koruma ve tespit sağlanmıştır.

### 1.3. Tezin Yapısı

Tez yedi ana bölümden oluşmaktadır.

İkinci bölümde insan bağışıklık sisteminin yapısı ve çalışma prensipleri üzerinde durulmuştur. İnsan bağışıklık sisteminin yapay bağışıklık sistemine adapte edilebilmesi için insan bağışıklık sisteminin iyi anlaşılması gerekmektedir. İnsan bağışıklık sisteminin fizyolojisi ve bu fizyolojiyi oluşturan öğelerin neler olduğu anlatılmıştır. Saldırı tespiti için gerekli olan lenfositlerin insan vücudu içerisindeki aktivasyonu ve tanıma, farklılaşma gibi aşamaları ne şekilde yapıldığı gösterilmiştir.

Üçüncü bölümde yapay bağışıklık sisteminin yapısı ve insan bağışıklık sisteminde bulunan mekanizmaların bilgisayar sistemlerine adapte edilirken kullanım şekilleri anlatılmıştır. YBS kullanılarak bir uygulama geliştirilirken kullanılacak yapı gösterilip, daha sonra bu uygulamalar için kullanılabilecek yapay bağışıklık algoritmaları üzerinde durulmuştur. Daha sonra yapay bağışıklık sistemi kullanılarak yapılan çeşitli uygulamalar gösterilmiştir. Sonrasında YBS' nin bilgisayar ağlarına uygulanma mimarisi hakkında bilgiler verilmiştir. Bilgisayar güvenlik sistemlerine yapay bağışıklık sisteminin uygulanma koşulları ve yapısı gösterilmiştir.

Dördüncü bölümde kablosuz ağlar ile kablolu ağlarda güvenlik unsurlarının neler olduğu, kablosuz ağlarda yapılabilecek bir saldırı tespiti ile kablolu ağlarda yapılabilecek saldırı tespit sisteminin ne gibi farklar içerdiği gösterilmiştir. Uygulamamızın temelini oluşturan kablosuz ağların kullanmış olduğu standartlar üzerinde durulmuştur.

Beşinci bölümde bilgisayar ağları için kullanılan saldırı tespit sistemleri sınıflandırılmıştır. Saldırı tespiti yapılırken seçilmesi gereken kriterlerin neler olduğu ve hangi saldırı tespiti sisteminin ne gibi avantaj ve dezavantajları olduğu gösterilmiştir.

Altıncı bölümde kablosuz ağlarda saldırı tespiti için kullandığımız yapay bağışıklık modelinin nasıl işlediği, oluşturulan modelin var olan saldırı tespit sistemlerine göre ne gibi avantajlar sağladığı gösterilmiştir. Ayrıca kullandığımız yapay bağışıklık algoritmasının ağ güvenliğine uygulanmış hali ve çalışma prensipleri anlatılmıştır. Kullanılan saldırı tespit

sisteminin, saldırıları nasıl tespit ettiği ve bu tespit sırasında hangi aşamalardan geçtiği gösterilmiştir. Bununla ilgili örnekler verilmiştir.

Yedinci bölümde uygulamamızın ağ ortamı tanıtılmış, kullandığımız yazılımın çeşitli parametrelerinin neler olduğu gösterilmiştir. Daha sonra uygulamamızın çeşitli sistem parametrelerinin değiştirilmesiyle elde edilen doğru tespit oranları ölçülmüş ve bu ölçüm sonuçları grafiklerle gösterilerek yorumlanmıştır.

Sekizinci bölümde çalışmamızdan elde ettiğimiz sonuçların neler olduğu, gelecekte bu konu ile ilgili yapılabilecek çalışmalar hakkında bilgiler verilmiştir. Ayrıca konuyla ilgili yapılmış olan çalışmaların neler olduğu anlatılmıştır.

# 2. BAĞIŞIKLIK SİSTEMİ

## 2.1. Genel Bilgiler

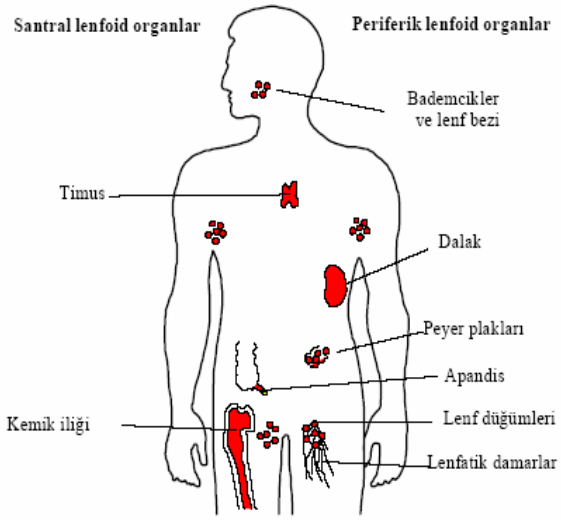
İnsan vücudu sürekli olarak dış çevreden gelen mikropların, virüslerin, bakterilerin saldırısına uğramaktadır. Bağışıklık sistemi, bu mikroorganizmaların vücuda zarar vermesini engellemek ve hızlı bir şekilde vücudu terk etmelerini sağlamak için gerekli işlemleri başlatır. Bu işlemlerin hepsine birden 'bağışıklık cevabı' adı verilir [1]. Sağlıklı bir vücut; karşılaştığı hastalık etkenleriyle ve yabancı maddelerle çoğunlukla bizim haberimiz olmadan baş eder. Vücut mikroplarla baş edemediği durumlarda da "hasta" olur. Bağışıklık cevabının gerçekleştiği süre içerisinde "hastalık" devam eder. Bu süre, mikroorganizmanın yapısına ve vücudun direncine göre farklılık gösterdiği için hastalık süreçleri de farklılık arz etmektedir. Bağışıklık cevabının sonunda vücut mikroorganizmayı yenmeyi başardıysa bu mikroorganizmaya duyarlı hücreler hafıza hücreleri olarak saklanır. Buradaki amaç, vücudun söz konusu mikroorganizmaya karşı bağışıklık kazanmasını sağlamaktır. Bağışıklık cevabında olumlu bir yanıt oluşmayabilir. Bu durumda hastalığın ilerlemesi söz konusudur ve vücut hastalıkla savaşmaya devam eder.

Bağışıklık sistemi, nörolojik sisteme benzer bir yapıya sahiptir. Bağışıklık sisteminin en önemli özelliklerinden biri; kendi hücreleri ile yabancı milyonlarca değişik düşmanı tanıyıp ayırt edebilme yeteneğine sahip olmasıdır. Bağışıklık sisteminin diğer bir özelliği de, hatırlama yeteneğine sahip olmasıdır. Bu özelliği sayesinde bağışıklık sisteminde görevli olan tüm hücreler, ilk karşılaştığı yabancıyı görür, belleğine kaydeder ve daha sonra gördüğünde de hatırlar. Bağışıklık sisteminin vücudu savunmada başarılı olmasının altında yatan sebep ise; vücudumuz içerisinde detaylı ve dinamik bir iletişim ağına sahip olmasıdır. Milyonlarca hücre bir araya gelip seriler halinde organize olur ve bilgileri arkadan ileriye doğru iletir [2]. Bir kez bağışıklık hücreleri uyarıyı aldıkları zaman, taktiksel birtakım değişiklere giderek çok güçlü kimyasallar üretmeye başlarlar. Bu maddeler hücrelerin kendi büyüme ve hareketlerini düzenlemelerine izin vererek vücut savunmasını başlatır.

Canlılar öldüğünde; bağışıklık sistemleri de (diğer her şeyle birlikte) yok olur. Saatler içerisinde vücudu çok çeşitli bakteri, parazit ve mikrop istila eder. Ancak bunların hiçbiri bağışıklık sistemi çalıştığı zaman vücuda giremez. Bağışıklık sistemi bozulduğu veya yok olduğu noktada, vücudun savunma kapıları sonuna kadar açık kalır. Bunun sonucunda da vücut alerji, artrit, enfeksiyonlar veya AIDS gibi birçok hastalığın gündeme geldiği durumlarla karşılaşabilmektedir.

## 2.2. Bağışıklık Sisteminin Fizyolojisi ve Temel Öğeleri

Bağışıklık yanıtının oluşmasından organizmadaki belli başlı bazı sistemler, organlar ve hücreler sorumludur. Bağışıklık sisteminin organlarına lenfoid organlar adı verilir. Lenfoid organlar santral (birincil) ve periferik (ikincil) olmak üzere ikiye ayrılır [3]. Santral organlar, yeni lenfositlerin antijene bağımlı olmaksızın otonom olarak yapıldıkları ve bağışık tepki oluşturma yeteneği kazandırdıkları yerlerdir. Periferik lenfoid organlar ise, lenfositlerin prolifere oldukları ve antijenik uyarılara tepki gösterdikleri yerlerdir [3].




**Şekil 2.1** Bağışıklık Sisteminin Anatomik Yapısı

*Lenf düğümleri:*

Vücudun birçok bölgesinde gruplar halinde bulunur. Boyun, koltuk altı, kasıklarda olduğu gibi yüzeyde bulunan lenf düğümleri kolaylıkla fark edilebilir. Ancak göğüs ve karın boşluğunda da çok sayıda lenf düğümü mevcuttur [4]. Bunların başlıca görevi vücuda giren yabancı maddelere karşı bir süzgeç oluşturarak, mikropların vücuda yayılımlarını engellemek ya da geciktirmektir. Düğümler içinde bağışıklık sistemine ait sayısız hücre bulunmakta, bu hücreler insana zarar verebilecek maddelerin geçişine engel olmaya çalışmaktadırlar. Bu mücadele sırasında lenf bezeleri şişerek elle ya da gözle fark edilebilecek boyutlara ulaşabilmektedir. Bademciklerimiz de birer lenf düğümüdür. Bakteriler ya da virüslerle yoğun bir biçimde savaştığında, bademciklerimiz şişer ve iltihaplanır.

*Timus:*

Göğüs boşluğu içinde yer alan iki parçadan oluşan bir organdır. Lenfosit, T lenfosit veya sadece "T hücreleri" timus' ta büyür, eğitilir, olgunlaşır ve bağışıklık sisteminde üstlendikleri görevleri yerine getirmek üzere yeniden kana karışırlar.

*Dalak:*

Sol böbreğin arka bölümünde yer alır. Kırmızı kan hücreleri ve bağışıklık sistemin beyaz kan hücreleri için depo olarak görev yapar, aynı zamanda kandaki yabancı maddelerin büyük bir kısmını süzer.

*Kemik İliği:*

Kemiklerin ortasında bulunan yağlı ve gözeli bir dokudur. Bağışıklık sisteminde çok önemli işlevleri olan akyuvarlar da dâhil olmak üzere bütün kan hücrelerinin yapım yeridir.

*Akyuvarlar:*

Akyuvarlar (Lökositler); bağışıklık sistemimizin en önemli savaşçıları ve immünolojik savunmanın temel elemanlarıdır. Lökositler damar içinde dolanırken, tehlike sinyallerini aldıkları bölgelerde damardan ayrılıp bakteri ve ölü doku gibi yabancı cisimlerin etrafını sarabilirler. Lökositler plazma kaynaklı kan proteinleriyle birlikte organizmanın bütünlüğünü sağlamakta askeri güç gibi görev yaparlar [4]. Bu savaşçıların da bakteri ve virüslerin yok edilmesinde çalışan farklı çeşitleri vardır. Bunlar;

- Granülositler
- Lenfositler
- Monosit ve Makrofajlar

Akyuvarların saldırı tespiti için kullanılan en önemli elemanları lenfositlerdir. İnsan vücudundaki saldırılara karşı cevap üreten organlar lenfositler olduğu için bu organlar üzerinde durulmuştur.

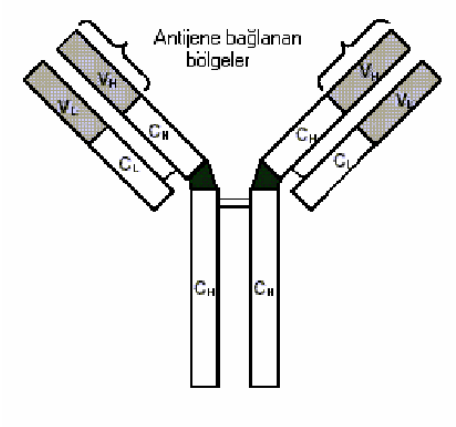
## 2.3. Lenfosit Tipleri

Bağışıklık sisteminin en önemli birimlerinden biri lenfositlerdir. İnsan vücudundaki saldırı tespitinde harekete geçen ve gerekli işlemleri yapan organları lenfositlerdir [5]. Lenfositlerin bu özelliklerinden dolayı saldırı tespit sistemlerinde lenfositler, bağışıklık cevabını oluşturan asıl birimlerdir. Lenfositlerin vücuttaki tanınan hücrelerle (öz hücreler) ve antijenlerle (öz olmayan hücreler) etkileşimi, yüzeylerinde bulunan reseptörler yardımıyla olur. Bu reseptörlerin değişiklik arz etmesi üç tip lenfosit'i karşımıza çıkarır. Bunlar T tipi lenfositler (T hücreleri), B tipi lenfositler (B hücreleri) ve doğal öldürücü (NK) hücrelerdir.

T tipi hücrelerin iki kısımdan oluşmaktadır. İlk kısım T hücreleri aktivatör görevi görürken ikinci kısım T hücreleri baskılayıcı olarak çalışır ve bu şekilde bağışıklık cevabının istenen seviyede olmasını sağlarlar. Aktivatör görevi yapan T hücreleri vücuda çeşitli kimyasallar yayarak bağışıklık cevabını direk oluşturur (CD8 CTL -T- lenfositleri ile) ya da oluşmasına katkıda bulunurlar (CD4 yardımcı T hücreleri ile). Baskılayıcı görevi yapan T

hücrleri ise çeşitli kimyasallar yayar ve bağışıklık cevabını oluşturmakta olan T ve B hücrelerinin çalışmalarını frenleyen bir etki gösterirler. T lenfositlerinin yüzeylerindeki reseptörlere TCR, CD4 ve CD8 adı verilir [5]. TCR, T lenfositlerinin antijenik yapılara bağlanmasını sağlar. CD4 ve CD8 reseptörleri ise bağışıklık yanıtı esnasında gerçekleşen etkileşimlerde görev alan ara reseptörlerdir [5].

B hücreleri, yüzeylerinde immunoglobin molekülleri taşırlar [2]. İmmunoglobin molekülleri birbirine benzer yapıda antikorlardan oluşur. Şekil 2.2' de görüldüğü gibi antikorlar, protein dizilimlerinin yer aldığı bir ağır zincir bir de hafif zincir' den oluşurlar. Antikorların V bölgeleri, antijenlerle ya da diğer antijenik yapılarla birleşme yerleridir. Bir birey yaklaşık 10 farklı çeşitte antikor üretebilir [1]. Antikorlar C bölgelerine göre beş farklı sınıfa ayrılırlar; IgM, IgD, IgG, IgE ve IgA' dır. Antikorların efektör fonksiyonlarının çoğu ağır zincirlerinin C bölgeleri ile başlar. Efektör fonksiyonlarının başlayabilmesi için de V bölgelerinin antijen reseptörlerine bağlanmaları gerekmektedir.




**Şekil 2.2** Antikor Yapısı

B hücreleri aktive olduklarında plazma hücrelerine dönüşürler ve yüzeylerinde bulunan immunoglobin moleküllerinden antikor salgılarlar. Salgıladıkları bu antikorlar antijenler ile birleşerek bir antijen-antikor yapısı oluştururlar. Bu yapının oluşması, çevreye bazı kimyasal sinyaller yayılmasını tetikler ve bu sinyalleri algılayan öldürücü hücreler bu yapıyı parçalayarak yok eder [2].

## 2.4. T ve B Lenfositlerinin Bağışıklık Sistemindeki Özellikleri

Bağışıklık sistemi mikroplara karşı bağışıklık kazanırken iki temel yapı kullanmaktadır. Bunlardan ilki doğum ortamında gelen doğumsal (*innate*) bağışıklıktır [5]. Bağışıklığın oluşmasında gözlemlenen bağışıklık çeşididir. Doğumsal bağışıklık, vücuda giren ya da girebilecek mikropların çoğunda ortak olan yapıların uyarımı ile başlamaktadır. Doğumsal bağışıklıktan sonra adaptif bağışıklık oluşmaktadır. Adaptif bağışıklık, farklı mikropsal ya da

mikropsal olmayan antijenler için özeldir. Adaptif bağışıklığın oluşum sürecinde gereken hücreler şunlardır: Antijen özellikli lenfositler, lenfosit aktivasyonu için gerekli yardımcı hücreler ve antijenleri yok etmek için efektör hücreler.

Vücuda dış ortamdan giren antijene karşı gösterilen bağışıklık yanıtı antijenin yapısına göre hücresel ve humoral bağışıklık olmak üzere ikiye ayrılır [4]. Humoral bağışıklık, hücre dışı mikroplara karşı görülür ve bu tür bağışıklık yanıtında *B* hücreleri aktiftir. Hücresel bağışıklık ise hücre içi mikroplara karşıdır ve sadece *T* hücreleri görev alır.

- *B* ve *T* lenfositlerinin temel farkları: Antijen reseptörleri ve fonksiyonlarıdır.
- Antijenler, antikorlara ya da *T* lenfositlerinin antijen reseptörlerine bağlanırlar. Antikorlara bağlanan antijenler; şekerler, lipitler, karbonhidratlar, proteinler ve nükleik asitleri içeren biyolojik moleküllerdir. *T* hücresi reseptörleri ise sadece peptid antijenleri tanırlar.
- *T* ve *B* lenfositleri, antijen ile karşılaştıklarında efektör hücrelere dönüşürler ve bağışıklık cevabında rol oynarlar. *B* hücreleri, Antikor salgılayan plazma hücrelerine dönüşürken; *T* hücreleri de sitokin salgılayan $CD4^{+}$ yardımcı *T* hücresine ya da $CD8^{+}$ salgılayan *CTL*' lere dönüşürler.

### 2.4.1. T ve B Lenfositlerinin Olgunlaşması, Aktifleşmesi ve Düzenlenmesi

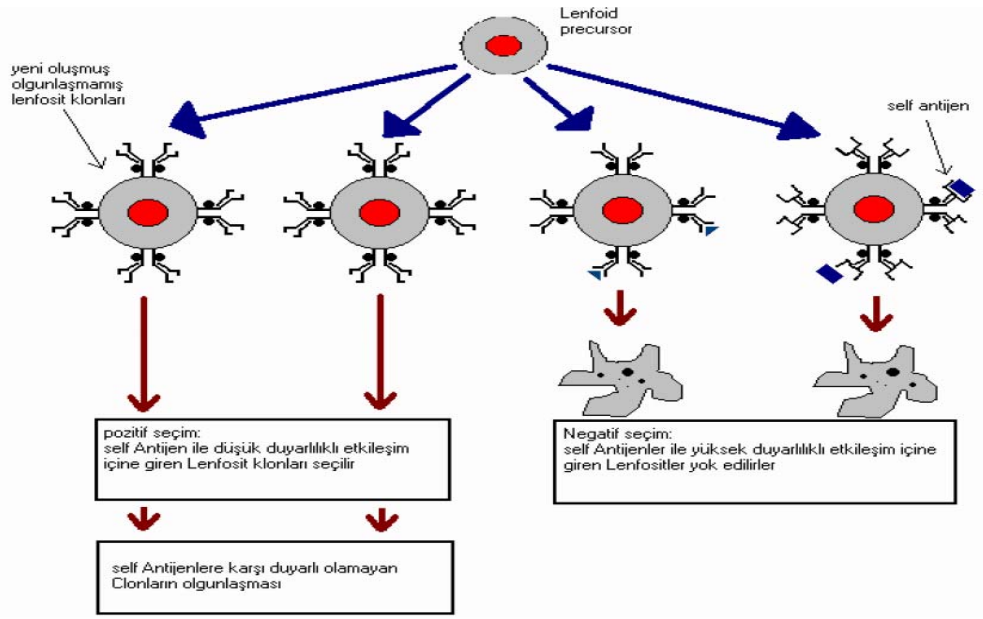
T ve B Lenfositlerin bağışıklık sisteminde görev yapabilmesi için çeşitli olgunlaşma evrelerini tamamlamaları gerekmektedir. Bu geçen zamandaki işlemlere olgunlaşma (maturation) adı verilir [5]. B ve T lenfositlerin üretimi insan vücudunda kemik iliğinde başlamaktadır. B hücresi, olgunlaşıp kullanılır hale gelmesine kadar geçen süreyi kemik iliğinde tamamlar. Fakat T hücresi olgunlaşma aşamasını tamamlamak için Timus' a geçer. Her iki hücre tipinin olgunlaşmasında göze çarpan önemli nokta, olgunlaşma esnasında yüksek ve hızlı bir bölünerek çoğalma işleminin olmasıdır. Bu da çok çeşitli bir repertuarın oluşmasını sağlamış olur. Burada repertuar ile kastedilen, B ve T lenfositlerinin çeşitliliğidir [6].

Fonksiyonel reseptör genleri, olgunlaşmamış B hücreleri için kemik iliğinde, T hücreleri için ise timus' ta üretilir. Olgunlaşmadaki bir diğer önemli nokta, olgunlaşma sırasında reseptörlerde meydana gelen gen farklılaşmasıdır [6]. Her bir B ve T lenfosit klonu, tek bir yapıda reseptör üretir ve bir bireyde $10^{9}$ ya da daha fazla farklı B ve T lenfosit klonu bulunabilir. Fakat gerçekte bu mümkün değildir. Çünkü böyle olması halinde vücuttaki hücrelerin çoğunluğu B ve T hücrelerinden (lenfositlerinden) oluşması gerekir. Bu durumda repertuar çeşitliliği, olgunlaşma esnasında gerçekleşen somatik farklılaşmalar ile gerçekleştirilir [7].

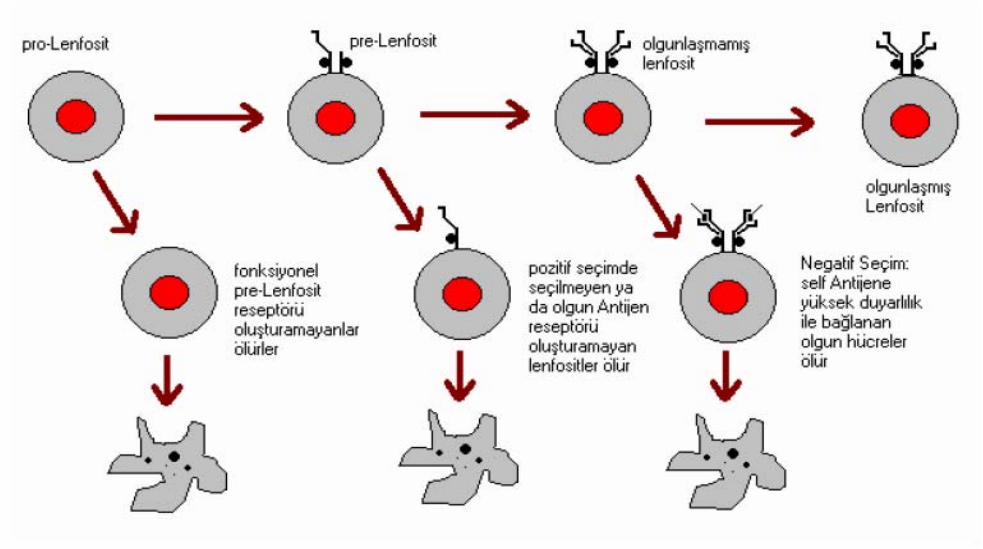
Lenfositlerdeki antijen reseptörleri, rasgele DNA farklılaşması ile üretilirler ve antijen varlığına bağlı değildirler. Bir başka deyişle, lenfosit reseptörleri, antijen ile karşılaşılmadan

üretilirler. Somatik farklılaşmadan sonra gerçekleşen en önemli olay, seçme işlemidir. Farklılaşma çoğunlukla başarısızlıkla sonuçlanır ve işe yaramayan birçok B ve T hücresi apoptosis adı verilen bir mekanizma ile ölür. Bu aşamalar Şekil 2.3' de gösterilmiştir.

Olgunlaşma işleminden sonra, hızlı bölünerek çoğalma ile üretilen hücrelerin ancak %10'dan azı ikincil lenfoid organlara ve dokulara (bağışıklık cevabının gerçekleştiği organlar) geçebilirler. Şekil 2.4' de lenfositlerin ölüm ve olgunlaşma aşamaları gösterilmiştir.



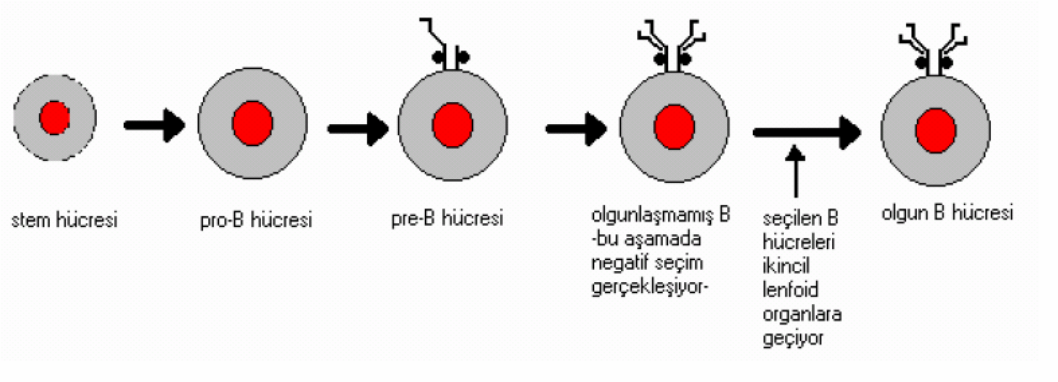

**Şekil 2.3** Lenfosit Olgunlaşmasındaki Seçim İşlemi




**Şekil 2.4** Lenfosit Ölümü ve Olgunlaşması

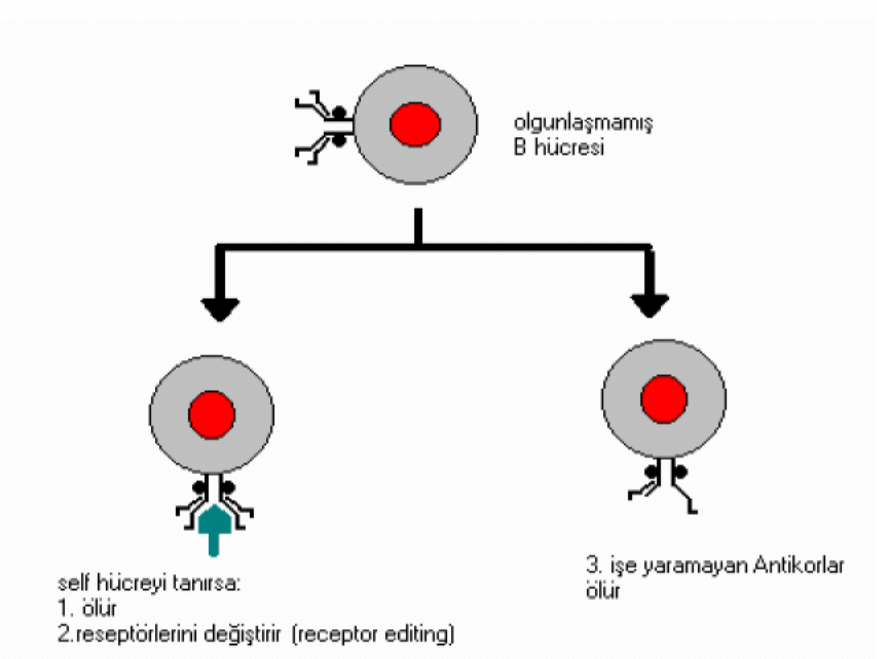
### 2.4.2. B Lenfositlerinin Olgunlaşması

Olgun B hücrelerinin yabancı antijenlere karşı çoğalarak yanıt üretmesi ikincil lenfoid dokularda gerçekleşir. B hücreleri bir kez uyarıldıktan sonra aktive olurlar ve salgılanmış haldeki Ig' lerin hücre duvarına bağlı Ig' lere oranı artar. Aktive olan B hücrelerinin bazıları da hafıza hücresine dönüşürler. Hafıza hücreleri uzun süreler hayatta kalır ve kan, lenf ve lenfoid organlarda aktif olarak dolaşım halinde bulunurlar. Hafıza hücrelerinin antijenler tarafından uyarılması, ikincil antijen yanıtlarının oluşmasına neden olur. İkincil yanıtlar hem süre hem de miktar bakımından ilk bağışıklık yanıtından daha etkindirler. Yaşamları süresince her bir B hücresi kopya üyeleri aynı V bölgesine sahiptirler ve aynı antijen özelliğinde kalırlar. Fakat antijene karşı yanıtlarda, antikorların V bölgelerinde açık değişimler meydana gelir. Antijenik uyarımdan sonra antijen özelliği artar [5]. Buna duyarlılık olgunlaşması adı verilir ve bu, humoral bağışıklığın bir karakteristiğidir [6]. Duyarlılık olgunlaşmasında V bölgelerinin DNA kodlamasında mutasyonlar gerçekleşir ve bu mutasyonları bir seçme işlemi takip eder. Böylelikle sadece yüksek duyarlılıklı hücreler hayatta kalır [7]. Şekil 2.5' de B lenfositlerinin olgunlaşması gösterilmiştir.




**Şekil 2.5** B Lenfositlerinin Olgunlaşması

Olgun B hücrelerinin seçimi, olgunlaşmamış hücrelerin arasından, bu hücreler kemik iliğini terk etmeden önce yapılır. Seçme aşamasında kemik iliğinde üç olay gerçekleşebilir Bu olaylar Şekil 2.6' da gösterilmektedir.

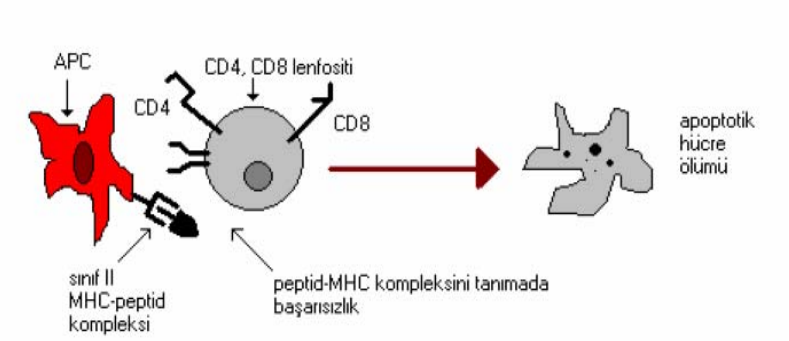



**Şekil 2.6** B Lenfosit Olgunlaşmasında Kemik İliğindeki Seçim İşlemi

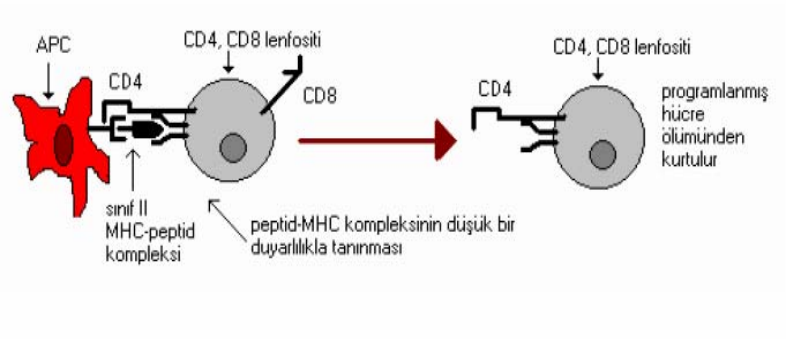
### 2.4.3. T lenfositlerinin Olgunlaşması

T hücrelerinin üretiminin kemik iliğinde başlamasına rağmen, T hücreleri olgunlaşma için Timus' a geçerler [1]. T lenfositleri sadece peptid antijenlerini tanırlar. Ayrıca bu peptid antijenleri ancak MHC moleküllerine bağlı ise tanıyabilirler. MHC molekülleri, antijen sunan hücrelerde bulunan ve peptid antijenlerini kendilerine bağlayan yapılardır. İki çeşit MHC molekülü vardır. Bunlar Sınıf I MHC ve sınıf II MHC' dir. Sınıf I MHC' lerin bağladığı antijenler $CD8^{+}$ CTL lenfositleri tarafından, sınıf II MHC 'lerin bağladığı antijenler ise yardımcı T lenfositleri tarafından tanınır.

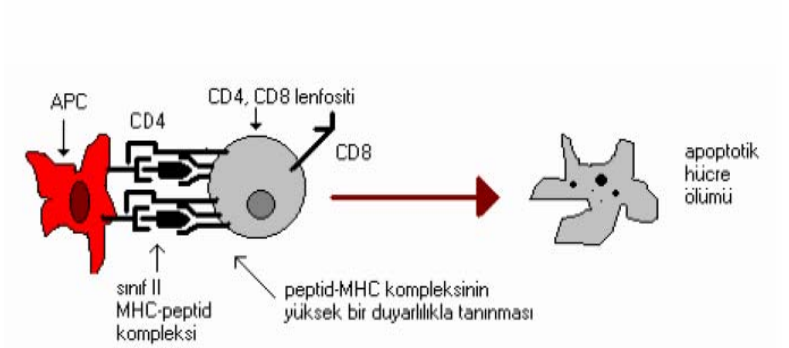
Timus' da iki çeşit seçim işlemi gerçekleşir; bunlar pozitif seçim ve negatif seçimdir. Şekil 2.7' de seçim işlemleri gösterilmektedir. Pozitif seçimde, tanınan peptid, MHC komplekslerine düşük bir duyarlılıkla bağlanan olgunlaşmamış T hücreleri hayatta kalmaları için bir uyarım alarak seçilmiş olurlar. Negatif seçimde ise, tanınan peptid, MHC komplekslerine yüksek bir duyarlılıkla bağlanan olgunlaşmamış T lenfositleri öldürülür [1]. Timus' da vücutta bulunan tanınan antijenlerin büyük çoğunluğu mevcuttur. Böylelikle, pozitif ve negatif seçim işlemleri ile vücut antijenlerine duyarlılığı fazla olan ve vücutta sirkülasyona katılması halinde vücuttaki tanınan antijenlere karşı bağışıklık yanıtın oluşmasına neden olabilecek olan T lenfositleri yok edilmiş olur [6].




(a)




(b)




(c)

**Şekil 2.7** Timus' da ki seçim işlemleri (a) Pozitif seçim eksikliği, (b) Pozitif seçim, (c) Negatif seçim

## 2.5. Tanıma, Çoğalma ve Farklılaşma

T Lenfositlerinin aktivasyonu için iki olay gerçekleşmelidir. Bunlar T hücresi reseptörlerinin (TCR' ler), MHC-peptid yapılarını tanımaları ve T hücrelerinin yardımcı molekülleri ile antijen sunan hücreler üzerindeki ligandların uyarılması gerekmektedir. Uyarılma, T hücresi aktivasyonu için "ikincil sinyaller" i sağlarlar. Uyarılma yoksa antijen ile karşılaşan T hücreleri ya apoptosis ile ölür ya da "anergy" adı verilen yanıtsızlık durumuna

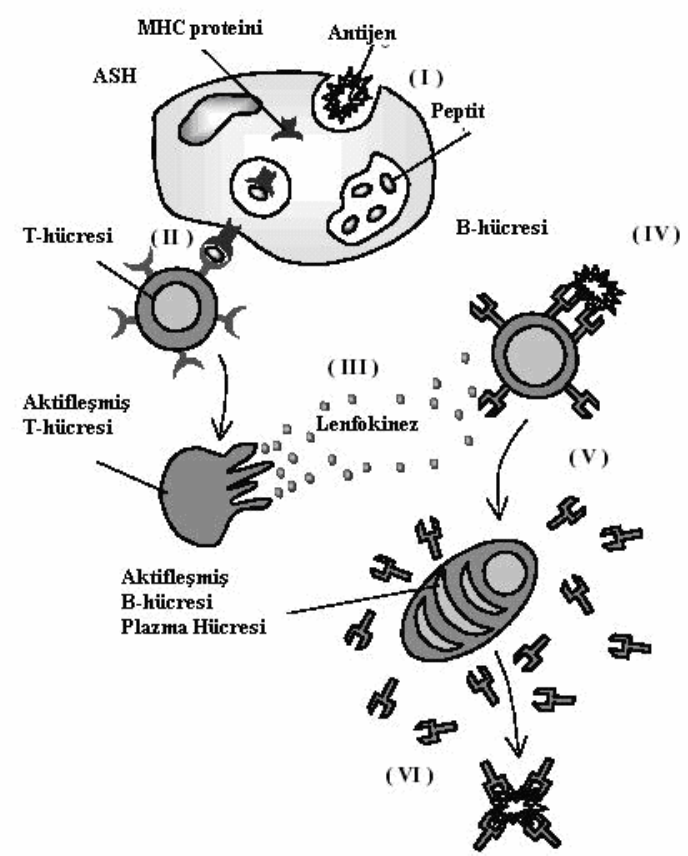
geçerler. Dolayısıyla uyarılma sayesinde T Lenfositlerinin yanıtları doğru zaman ve doğru yerde başlatılmış olur [5].

T hücresi ve antijen tanınmasının sonucu, TCR-antijen etkileşiminin süresi (ya da yarı ömrü) ve duyarlılığı ile belirlenir. TCR' lerin peptid-MHC yapısı halindeki antijenlere olan duyarlılıkları, çoğu antikorun antijenlere olan duyarlılıklarına göre oldukça düşüktür. TCR-antijen etkileşiminin düşme oranı çok hızlıdır. Tek bir TCR' nin MHC bağımlı peptidi 10 saniyeden az meşgul ettiği hesaplanmıştır [4]. Bir T hücresinin aktivasyonu için etkileşim esnasında birçok sıralı olay meydana gelmelidir. Bu nedenle T hücresi, TCR reseptörlerinin peptid-MHC yapılarına bağlanış sayısını ve süresini toplayan bir sinyal toplayıcı (integratör) gibi davranır. Aktivasyonun olabilmesi için, TCR kaynaklı sinyallerin bir eşik seviyesine ulaşması gerekmektedir. Bu eşik seviyesi aşılamazsa; ya bir yanıt üretilmez, ya da sadece bazı yanıtların üretildiği bir yarı aktivasyon gerçekleşir. Hafıza ve ejektör T hücrelerinin aktivasyonu için gerekli eşik seviyesi, olgun T hücrelerinden daha azdır [6].

Olgun T hücrelerinin çoğalmasına "klonal genişleme" denir. Bunun sonucunda antijeni elemek için gerek duyulan antijen özellikli hücrelerden oluşan bir popülasyon meydana gelir. Olgun T hücrelerinin farklılaşması, olgun T lenfositlerinin efektör hücrelere dönüşmesi işlemidir. Bu işlem, hem T hücresinin antijen ile indüklenen aktivasyonunu hem de diğer uyarımları gerektirir. Burada bahsedilen diğer uyarımlar, genelde antijen tanınma tarafında üretilen interlökin 2 (IL-2) adı verilen salgılardır [7].

### 2.6. Bağışıklık Sisteminin Çalışma Mekanizması

Bağışıklık sistemi organları ve yapısı gösterildikten sonra bağışıklık sisteminin çalışma mekanizması özet olarak şöyle açıklanabilir. Bağışıklık sistemi, vücudumuzu enfeksiyonlara karşı koruyan bir grup hücreden oluşmaktadır. Vücudumuz sürekli olarak antijenlerin saldırılarına maruz kalmaktadır. Bu antijenler yabancı hücreler olabileceği gibi vücudumuzun kendi hücresi de olabilir. Şekil 2.8' de temel bağışıklık tanıma sistemi ve aktivasyon mekanizması gösterilmektedir [2].




**Şekil 2.8** Bağışıklık Sisteminin Çalışma Mekanizması

**I.** Antijen sunucu hücrelerin nasıl özelleştiği gösterilmektedir. Bu antijenler peptidlerine ayrılır.

**II.** Peptid molekülleri MHC moleküllerine bağlanırlar. ASH hücresi içinde bunlar MHC/Peptid bileşimi şeklinde bulunur.

**III.** T-hücreleri yüzeylerinde reseptörler yardımıyla farklı MHC/Peptid bileşimlerini tanırlar.

**IV.** MHC/Peptid bileşiminin tanınmasıyla aktif hale gelen T-hücresi, parçalanarak, lenfokin ve kimyasal salgılar. Bu salgılar bağışıklık sisteminin diğer bileşenleri de aktif hale geçmesini sağlar.

**V.** B-hücreleri, T-hücrelerinden farklı olarak antijenleri MHC moleküllerinin yardımı olmadan da reseptörleri yardımıyla tanıyabilir.

**VI.** B-hücrelerinin yüzeyindeki reseptörler belli bir antijene cevap verebilecek şekildedir. B-hücrelerinden reseptörleri bu şekilde bir antijene yanıt verdiğinde diğer B hücreleri aktif hale geçmekte ve farklılaşarak plazma hücrelerini oluşturmaktadır. Daha sonrada antikor molekülleri salgılar.

**VII.** B-hücreleri reseptörleri tarafından çözülebilecek formda olan antikorlar zararlı maddelerin yok edilmesinde kullanılır. Bazen aktive edilmiş bu B hücreleri ve T hücreleri hafıza hücrelerine dönüşür.

# 3. YAPAY BAĞIŞIKLIK SİSTEMİ

## 3.1. Yapay Bağışıklık Sisteminin Tarihi

Yapay Bağışıklık Sistemleri birçok araştırmacı için yenilikler teşkil etmektedir. Özellikle ağ güvenliği konusunda elde edilen olumlu sonuçlardan dolayı yapay bağışıklık sistemlerinin kullanımı yaygınlaşmıştır. Bağışıklık biliminin başlangıcı Edward Jenner' in aşıyı bulduğu 1976 yılına dayanmaktadır. Bu tarihten günümüze kadar Bağışıklık alanında yapılan keşifler, Bağışıklık Sisteminin işleyişindeki çoğu karanlık noktayı aydınlatmıştır. Bağışıklık Ağı Teorisi ile Niels K. Jerne 1974 yılında, reseptör çeşitliliği ve yapısal bağışıklık üzerine yaptığı çalışmalar ile de Susumu Tonegawa 1983 yılında Nobel ödülüne layık görülmüştür. Bağışıklık biliminde yapılan çalışmalara paralel olarak oluşturulmaya başlanan Bağışıklık Sistemi modelleri, sistemin işleyişini kavrama açısından oldukça büyük katkılar sağlamışlardır.

1900'lü yılların ikinci yarısından itibaren gelişmeye başlayan Yapay Zeka, insan gibi düşünen ve davranan makinelerin ortaya çıkarılması gibi amaçlara yönelik çalışmalarda büyük ölçüde insanın biyolojik sisteminin işleyişini referans almıştır. Bu alanda en çok kabul gören ve Yapay Sistemlerde bir çığır açan Yapay Sinir Ağları, uygulama alanını sadece insanı taklit eden makinelerin oluşturulması ile sınırlı tutmamış, bilimin birçok alanında karşılaşılan karmaşık problemlerde başvurulabilir etkin bir çözüm sistemi olarak kendini ispatlamıştır. Sinir sistemindeki bilinen işleyişleri model alarak oluşturulmaya başlanan Yapay Sinir Ağları'nın böylesi ses getirmesi şaşırtıcı değildir çünkü insandaki biyolojik sistem, bilinen işleyişi ile bile çok karmaşık bir mükemmellik arz etmektedir [1]. Bağışıklık sistemindeki olayların aydınlatılmaya başlanması ve Yapay Zeka' ya duyulan ilginin artması, Yapay Bağışıklık Sistemlerinin ortaya çıkışının ardında yatan temel nedenler arasında yer almaktadır. 1974 yılında Jerne' nin ortaya attığı Bağışıklık Ağı Teorisi ve Bağışıklık Sistemindeki işleyişleri daha anlaşılabilir kılan Bağışıklık Sistemi Modelleri, Yapay Zeka araştırmacılarının ilgisini çekmiş ve oluşturulan yeni algoritma ve uygulamalarla Yapay Bağışıklık Sistemleri yavaş yavaş adından söz ettirmeye başlamıştır. Gelişiminin Yapay Sinir Ağları kadar hızlı olmaması ve o kadar çok ilgi toplamamış olmamasına karşın son yıllarda bu durum değişmeye başlamıştır. Özellikle 1990'lı yılların sonlarından itibaren Yapay Zeka alanında çalışmakta olan çoğu araştırmacı, dikkatini Yapay Bağışıklık Sistemlerine yöneltmiş ve bu alanda en az Yapay Sinir Ağları kadar etkin yeni algoritmalar oluşturulmaya başlanmıştır [8].

Yapay Bağışıklık Sistemlerinin uygulama alanları şu şekilde özetlenebilir: Saldırı tespit sistemleri, robotik, kontrol, optimizasyon, yapay sinir ağı yaklaşımları, anormallik tespiti, etmen tabanlı yaklaşımlar, öğrenme, indüktif problem çözme, örüntü tanıma, bilgisayar modelleri,

diğer yaklaşımlar (Açık Web sunucusu koordinasyonu, listeleme, veri madenciliği, sınıflama sistemleri, sensör tabanlı teşhis, gen kütüphanelerinin gelişimi, öz-tanıma işlemi ) şeklindedir.

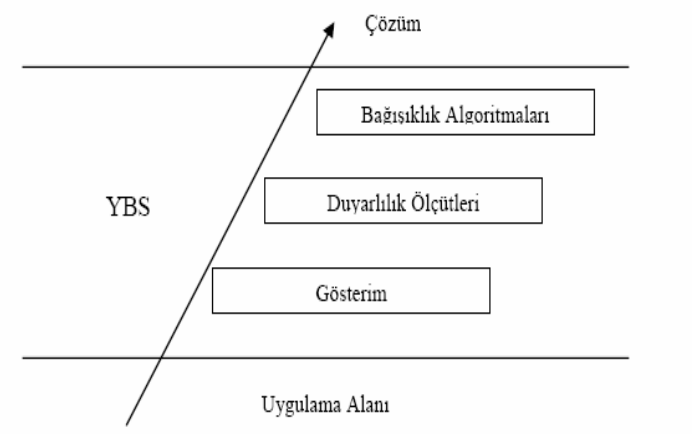
Son yıllarda Yapay Bağışıklık Sistemleri üzerinde çalışmalar yapan araştırmacılar arasında D. Dasgupta, J. Timmis, S.Forrest, S. Hofmeyr, L. N. De Castro, F. J. Von Zuben, A. B Watkins, J. Kim, T. Knight, Jean-Yves Le Boudec, Slavisa Sarafijanovic ve M. Neal oldukça etkili algoritmalar oluşturmuşlardır. Böylece Yapay Bağışıklık Sisteminin gelişmesine ve giderek daha fazla ilgi toplamasına sebep olmuşlardır [10-14, 24-26].

### 3.2. Yapay Bağışıklık Sistemi Tasarım Kriterleri

Bağışıklık sisteminden esinlenerek bir YBS oluşturmak için çeşitli tasarım ölçütlerine ihtiyaç duyulmaktadır. YBS tasarımına geçmeden önce bu kriterler göz önünde bulundurulmalı ve sistemin yapay bağışıklığa uygun olup olmadığına bakılmalıdır. Bu ölçütler aşağıdaki şekildeki gibi sıralanabilir;

- Sistemi oluşturan birimlerin gösterimi
- Sistemdeki birimlerin birbirleri ve çevre ile olan etkileşimlerini hesaplamak için bir mekanizma
- Bazı adaptasyon prosedürleri

Bir YBS tasarımında öncelikle sistemi oluşturan birimlerin Bağışıklık Sisteminin hangi elemanlarının modellenmesinden ortaya çıkacağının belirlenmesi gereklidir [9]. Sonrasında bu birimlerin sistemdeki diğer birimlerle ve çevre ile olan etkileşimlerinin türü ve boyutunun hesaplanmasında kullanılacak bazı duyarlılık ölçütleri oluşturulmalı ya da kullanılmalıdır. Son olarak ta sistem birimlerinin fonksiyonlarını belirleyen ve sistem birimlerinin hangi durumlarda nasıl davranması gerektiğini karakterize eden bir takım adaptasyon prosedürleri kullanılmalıdır.



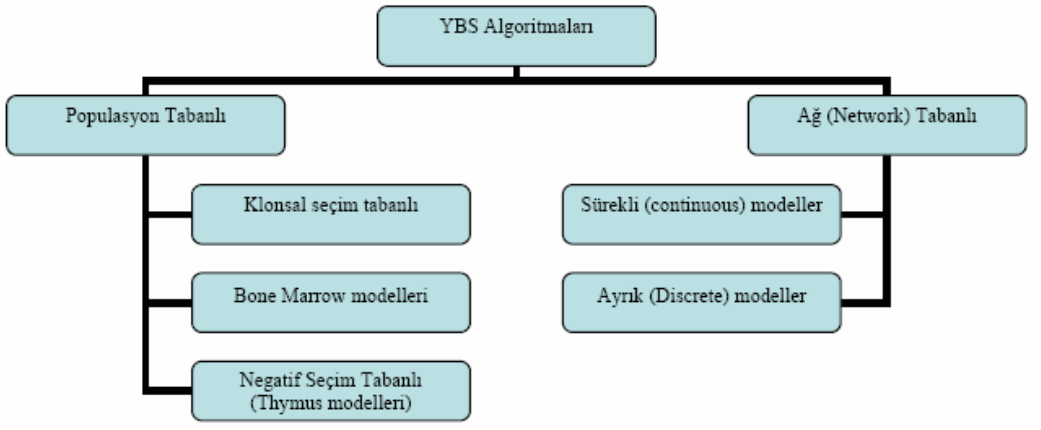

**Şekil 3.1** Yapay Bağışıklık Sisteminin Katmanlı Gösterimi

Yapay Bağışıklık Sistemleri alanında oluşturulacak her sistemin temelini uygulama alanı oluşturmaktadır. Uygulama alanının karakteristiğine uygun bir gösterim seçilerek duyarlılık ölçütleri de bu gösterimler temel alınarak oluşturulmalıdır. Gösterim şekli ve duyarlılık ölçütleri belirlendikten sonra oluşturulacak bağışıklık algoritmaları yukarıda da bahsedildiği gibi sistem birimlerinin fonksiyonlarını belirler. Örneğin bir tasarımcı anormal durum tespiti problemi için bir YBS sistemi oluşturmak istemektedir. Tasarımcı öncelikle bir gösterim şekli belirlemelidir. Bunun için bağışıklık sistemindeki antikorları sistem birimleri olarak ifade etmeyi seçebilir ve bu antikorların her birini ikilik diziler yardımıyla ifade edebilir. Bu durumda tasarımcının seçmiş olduğu gösterim şekli ikilik dizilerdir ve duyarlılık ölçütlerini bu gösterim şeklini dikkate alarak belirlemelidir. Tasarımcının belirleyeceği duyarlılık ölçütü ikilik diziler söz konusu olduğu için "r-ardışık bit kuralı" olarak seçilebilir. Son ve en önemli aşama olan bağışıklık algoritmasının oluşturulmasında ise tasarımcı bağışıklık sistemindeki bazı mekanizmaları seçmiş olduğu gösterim şekli ve duyarlılık ölçütünü dikkate alarak modelleyebilir. Bu modellemeler bire bir bağışıklıktaki bazı mekanizmaları kullanabileceği gibi bu mekanizmalardan esinlenilerek oluşturulmuş ve sadece bağışıklık mekanizmalarından oluşmayan modellemeler de olabilir. Örneğin bağışıklık sistemindeki duyarlılık olgunlaşması mekanizmasından yola çıkılarak bir bağışıklık algoritması oluşturulabilir [9, 10].

Yapay Bağışıklık Sistemleri alanında, yukarıda anlatılan işlemlerin her biri için çeşitli yöntemler geliştirilmiştir. Sistemin oluşmasında ilk yapılması gereken iş olan sistemi oluşturan birimlerin gösterimi için Perelson ve Oster' in 1979 yılında ortaya attıkları şekil-uzayı yaklaşımı, en çok kabul gören ve kullanılan yaklaşımdır [11]. Antikor ve antijen arasındaki etkileşimler de duyarlılık ölçütünün kullanılması aşamasında en çok tercih edilen modellemelerden birisidir. Bu alanda klonal seçim algoritması [10], negatif seçim algoritması [12], pozitif seçim algoritması [13], bağışıklık ağları, değişik uygulama alanları için oluşturulmuş ve oldukça çok kullanılan yöntemlerdir [14].

### 3.3. Yapay Bağışıklık Algoritmaları

Bir Yapay Bağışıklık sistemi tasarımında uygulama alanının yapısına uygun olarak seçilen gösterim şekli ve duyarlılık ölçütleri belirlendikten sonra sistemin çatısını oluşturacak olan bağışıklık mekanizmalarının modellendiği adaptasyon prosedürleri, başka bir ifade ile yapay bağışıklık algoritmaları oluşturulmalıdır. Günümüze değin yapılan çalışmalarda YBS alanının kısa bir tarihçesinin olmasına karşın oldukça fazla YBS algoritması karşımıza çıkmaktadır. Geliştirilen bu algoritmaları uygulama alanlarına ve yapılarına göre kategorize etmek mümkündür.




**Şekil 3.2** YBS Algoritmalarının Kategorileri

Şekil 3.2' de görüldüğü gibi geliştirilen YBS algoritmaları 2 temel kategoride toplanmaktadır [1]. Bunlar popülasyon tabanlı ve ağ tabanlı YBS algoritmalarıdır. Popülasyon tabanlı algoritmalar da kendi içerisinde Klonal seçim tabanlı, kemik iliği modelleri ve negatif seçim tabanlı olmak üzere üç gruba ayrılmaktadırlar. Ağ tabanlı algoritmalar ise sürekli modeller ve ayrık modeller olarak iki gruba ayrılmaktadır. Saldırı tespit sistemlerinde kullanılan algoritmalar popülasyon tabanlı algoritmalardır. Bu algoritmalardan en etkin ve kullanışlı olan algoritmaların başında negatif seçim algoritması gelmektedir. Çalışmanın temelini negatif seçim algoritması oluşturmaktadır.

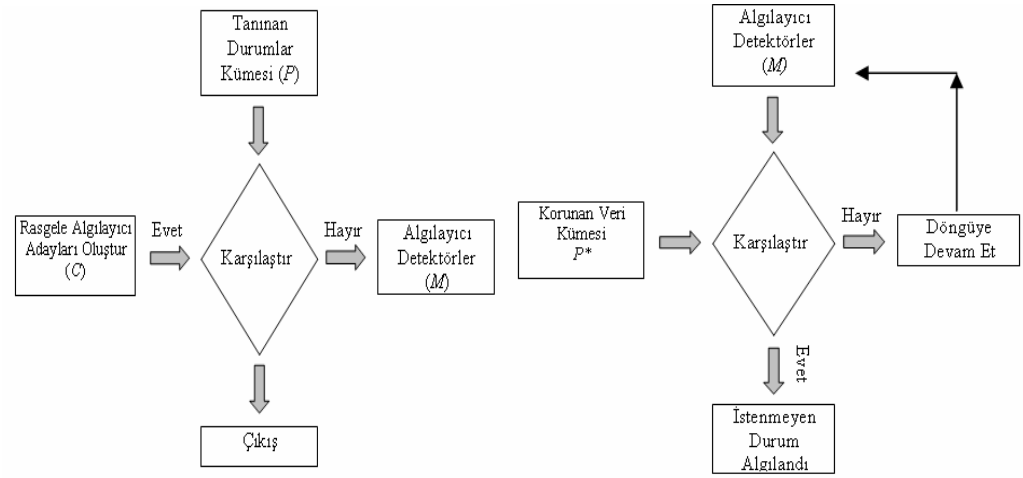
### 3.3.1. Negatif Seçim Algoritması

Timus, T hücrelerinin olgunlaşmasından sorumludur. Yabancı antijenleri timük çevrenin dışında tutan bir kan bariyer ile korunmaktadır. Bu nedenle timüs içinde bulunan çoğu eleman yabancı değil vücudun kendisine ait elemanlara örnek teşkil eder. T hücrelerinin timustaki gelişimleri esnasında timustaki kendisine ait antijenleri tanıyabilen algılayıcıları içeren T hücreleri, negatif seçim denen bir süreç ile T hücreleri repertuarından silinirler. Timustan ayrılıp vücudu dolaşan tüm T hücreleri öz' e karşı toleranslı olarak adlandırılır. Bir bilgi işleme perspektifi ile olaya bakılırsa, negatif seçim, desen tanımayı gerçekleştirmek için alternatif bir yöntem olarak karşımıza çıkmaktadır. Bu yöntem tanınacak durumları, tamamlayıcı küme hakkında bilgi depolama mantığı ile çalışır. Bilgisayar ve ağ saldırıları, zaman serileri tahmini, şekil denetimi ve kesimlemesi ve donatım hatası toleransı gibi anormallik belirleme problemleri ile ilgili uygulamalarla birlikte bir negatif seçim algoritması önerilmiştir [11–13]. Öncelikle, korunacak modellerin kümesi belirlenir ve *'öz set'(P)* olarak adlandırılır. Negatif seçim algoritmasına dayanarak, 'öz-set' kümesine ait olmayan elemanları

tanımakla sorumlu bir algılayıcılar *(detektörler) (M)* kümesi oluşturulur. Negatif seçim algoritmasının çalışma yöntemi Şekil 3.3' de verilmiştir [15].

**1.** Aynı gösterim kabulünü kullanan rasgele aday elemanlarını (*C*) oluştur.

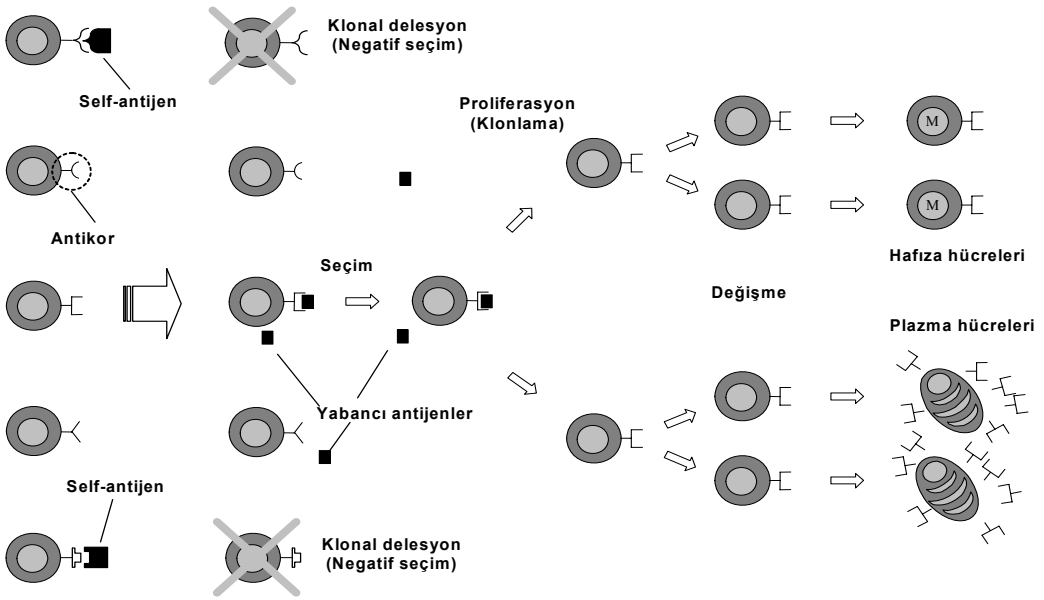
**2.** *C'* deki elemanlarla *P*' deki elemanları karşılaştırılır. Bir eşleşme olursa, örneğin, *P*' nin bir elemanı *C*' nin bir elemanı tarafından tanınırsa, *C*' nin bu elemanını atılır. Tersi durumda, *C* nin bu elemanını algılayıcı (detektör) kümesi içinde saklanır. Algılayıcı kümesini (*M*) oluşturduktan sonra, algoritmanın diğer aşaması tanınmayan modellerin varlığı için sistemi izlemekten oluşur. Bu durum Şekil 3.3 (b)' de gösterilmektedir. Bu durumda bir *P** korunacak kümesi oluşturulur. Bu küme, *P* kümesi ve diğer yeni modellerden veya tamamıyla yeni bir kümeden meydana gelir. Tanınmayan modellerine karşılık gelen, algılayıcı kümesinin tüm elemanları için, *P** kümesinin bir elemanını tanıyıp tanıyamadığı (eşleşme) kontrol edilir. Eşleşme var ise, o zaman bir tanınmayan modeli tanınmıştır ve reaksiyon başlamalıdır. Tanınmayan tespitinde sonuç aksiyonu değerlendirme problemine göre çeşitlilik gösterir ve negatif seçim algoritmasının model tanıma kapsamı dışındadır [14].




**Şekil 3.3 a)** Detektör Kümesi Oluşturma İşlemi **b)** Normal Olmayan Durum Tespiti

### 3.3.2. Klonal Seçim Algoritması

Klonal seçim algoritması, negatif seçimin rolünü tamamlayıcı olarak, bir "öz olmayan" hücre bir "B" hücresi tarafından tanındığı zaman nasıl bir bağışıklık tepkisi verileceğini açıklamak için kullanılmaktadır [10]. Şekil 3.4' de klonal seçim algoritmasının çalışması gösterilmektedir.




**Şekil 3.4** Klonal Seçim Mekanizması

Vücutta istenmeyen bir antijen tespit edildiği zaman, kemik iliğinden antikor üretilerek bağışıklık tepkisi veren B lenfosit hücreleri salgılanır. Bu antikorlar, antijenlerle birleştiği zaman yardımcı-T hücrelerinden gelen sinyallerin de etkisi ile B-hücresini uyarır. B-hücresi uyarma ile birlikte çoğalır ve plazma hücreleri denilen terminal antikor salgılayan hücrelere dönüşür. Hücre bölünmesi süreci bir kopya oluşturur. Bu kopya bir tek yavru hücre veya bir küme yavrudur.

Beyaz plazma hücreleri en aktif antikor salgılayıcılarıdır. Ayrıca, hızlı şekilde bölünen büyük B lenfositleri de daha düşük bir oranda antikor salgılarlar. Lenfositler çoğalma ve plazma hücrelerine dönüşmenin dışında uzun ömürlü B hücrelerine dönüşebilirler. Hafıza hücreleri kan, lenf, dokular boyunca dolaşır ve ikinci bir antijenik durumla karşılaşıldığında yüksek benzerlikte antikorlar üretme kabiliyetinde olan büyük lenfositlere dönüşebilir [17]. Bağışıklık sisteminin en önemli özelliği kuşkusuz öğrenmedir. Bağışıklık sistemindeki öğrenme, antijenleri tanıyarak kendini kanıtlayan lenfositlerin göreceli popülasyon büyüklüğünü ve antijenlere olan benzerliklerini artırmalarını içerir [17].

Normal bir bağışıklık sistemi evriminde, organizma, bir antijen ile hayatı boyunca defalarca karşılaşır. Bir antijen saldırısına ilk tepki her biri farklı benzerlik derecesinde antikor üreten, düşük benzerlik değerine sahip B hücreleri tarafından verilir. Bağışıklık sisteminin 2. saldırıya verdiği tepkinin etkinliği ilk enfeksiyon sonucunda oluşan hafıza hücrelerinin varlığı ile artırılır. Hafıza hücreleri, yüksek benzerlikte antikor üretebilirler. Bu strateji ile her

enfeksiyondan sonra bağışıklık tepkisinin sürati ve doğruluğu artar. Bu mutasyon ve seçim algoritmasını defalarca tekrar ederek, bağışıklık sistemi yüksek benzerlikteki antikorları üretmeyi "öğrenir". Bu olay; sistemin yeteneğini sürekli olarak artırmayı sağlayan bir destekli öğrenme stratejisidir [17,18]. Klonal seçim; Charles Darwin' in evrim teorisin in üç temel fonksiyonu olan farklılaştırma, çeşitlendirme ve doğal seçim mekanizmalarını kullanır. De Castro ve Von Zuben [17, 18], bu mekanizmaya göre optimizasyon problemleri için aşağıdaki algoritmayı (CLONALG) ortaya koymuşlardır. Şekil 3.5' de algoritmanın adımları gösterilmiştir.

**1**. Optimize edilecek bir *g(.)*, amaç fonksiyonu bulunmaktadır. Bir antikorun benzerlik değeri, verilen antikor için hesaplanan amaç fonksiyonunun değerine karşılık gelir: her bir *Abi* antikoru, girdi kümesinin (*Ab*) bir elemanıdır.

**2**. Her bir *Abi* için f benzerlik değeri (amaç fonksiyon değeri) hesaplanır.

**3**. En yüksek benzerliği (en yüksek uygunluğu) gösteren n tane antikor Ab kümesinden seçilir ve yeni bir *{ } n Ab* kümesi oluşturulur.

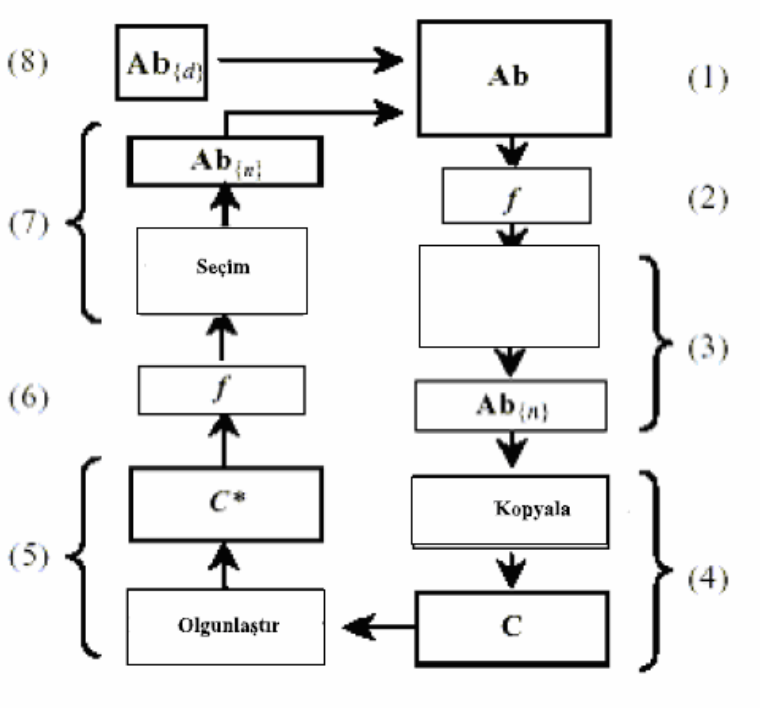
**4**. Seçilen n tane antikor bağımsız olarak ve antijenik benzerlikleriyle orantılı olarak klonlanır (kopyalanır), klonlar bir *C* repertuarı oluşturur: seçilen n antikorun her biri için oluşturulan kopya sayısı f benzerlik değeri ile orantılıdır. Daha yüksek antijenik benzerlik (daha yüksek uygunluk değeri), daha fazla sayıda kopya demektir.

**5.** C repertuarı, antijenik benzerlik ile ters orantılı olarak olgunlaştırma (hiper mutasyon) sürecine uğratılır. Bu süreç sonunda olgunlaştırılmış kopyaların oluşturduğu bir *C**; mutasyona uğratılmış kopyalar popülasyonu oluşturulur. Kopyaların mutasyona uğratılma oranı benzerlik değerleri ile ters orantılıdır: Daha yüksek benzerlik (daha yüksek uygunluk değeri), daha az mutasyon oranı demektir.

**6**. Mutasyona uğratılmış *C** kopyalarının benzerlik (uygunluk) değerleri hesaplanır.

**7**. En yüksek uygunluk değerine sahip n tane antikor yeniden seçilir ve *Ab* kümesine eklenir.

**8**. Son olarak, *Ab* kümesinden en düşük benzerlik değerine sahip d tane antikor, yeni oluşturulmuş antikorlar ile değiştirilir.




**Şekil 3.5** Klonal Seçim Algoritması Akış Diyagramı

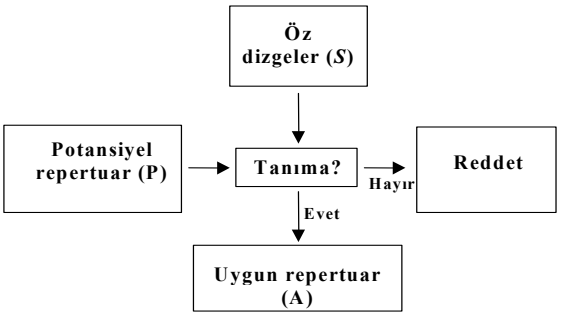
### 3.3.3. Pozitif Seçim Algoritması

Şekil 3.6' da pozitif seçim algoritmasının akış şeması gösterilmektedir. Çalışma mekanizması şu şekilde özetlenebilir:

**1. Başlangıç:** Olgunlaşmamış *T* hücrelerinin potansiyel repertuarını, *P*, üret. Tüm molekülleri (reseptör ve MHC' ler) aynı uzunluklu, L, ikili dizgeler ile temsil edildiğini varsayıldığında *2L* ayrı hücre üretilir.

**2. Benzerlik değerlendirmesi:** *P*' deki tüm elemanların öz hücre kümesi *S*' deki tüm elemanlar ile benzerliği belirlenir.

**3. Uygun repertuarın üretimi:** *P*' nin bir elemanı ile MHC' nin en az bir elemanı arasındaki afinite verilen çapraz reaktif eşiği e 'den büyükse ya da buna eşitse o zaman *T* hücresi bu MHC 'yi tanır. Pozitif olarak seçilir ve sisteme tanıtılır.(uygun repertuar A' ya); değilse T hücresi elimine edilir [12].




**Şekil 3.6** Pozitif Seçim Algoritması Akış Şeması

### 3.4. Yapay Bağışıklık Sisteminin Uygulama Alanları

**1-** Yapay bağışıklık sisteminin uygulama alanlarından biri de optimizasyon problemleridir. De Castro ve Zuben [17, 18] optimizasyon problemleri için kendilerinin önerdiği CLONALG algoritmasını kullanmışlardır. CLONALG algoritmasını 30 şehirli bir gezgin satıcı problemine uygulamışlardır. Problem için çalışmada bir tam sayılı şekil uzayı kullanılmıştır. L uzunluğundaki tamsayı değerli vektörler, C={1,2,...,L} elemanlarının permütasyonlarından oluşur ve bu vektörler mümkün turları belirtirler. Tamsayı vektörünün her bir bileşeni bir şehri gösterir. Her bir turun toplam uzunluğu, bir tura karşılık gelen vektörün benzerlik ölçüsünü verir. Mutasyon basitçe, turları belirten antikorlar içindeki şehir çiftlerinin yerlerini değiştirmek ile sağlanır. Çalışmada, Moscato ve Fontanari [19] tarafından ele alınan problem YBS ile çözülmüştür. Popülasyon büyüklüğü (antikor popülasyonu) 300 bireydir. Her 20 nesilde bir, antikorların en kötü %20'lik kısmı yenileri ile yer değiştirir. Algoritma 300 adım sonra, optimal sonuca ulaşmıştır. Costa ve diğ. [20] 'de, paralel makineler de toplam tamamlanma zamanının en azalması problemi üzerinde durmuşlardır. Çalışmada CLONALG algoritması üzerine kurulan bir yapay bağışıklık sistemi modeli ile bazı sezgiseller karşılaştırılmıştır. Karşılaştırılan sezgiseller; LPT, Multifit, Lokal Arama ve Tavlama Benzetimidir. Problem için her olurlu çözüm, örneğin tam bir çizelge, sabit *n* büyüklüğünde bir dizi olarak kodlanmıştır. Dizi üzerindeki her pozisyon bir süreç ile ilişkilidir. Her *i* pozisyonunun değeri işlemin yerleştirileceği makineyi belirtir. Popülâsyonun her bir antikoru (çözümü) için bir benzerlik (affinity) değeri vardır.

Aşağıdaki denklemde gösterilen bu benzerlik değeri, çözümün kalitesini yansıtır:

LB Benzerlik(k)  (1+M(k) - LB)' dır.

Burada; *M(k); k* antikoru ile gösterilen çözümün toplam tamamlanma zamanını gösterir. *LB;* problemin alt limitini belirtir. Bu alt limit, tüm işlem zamanları toplamının işlemci sayısına

oranı ile bulunur. Denklemdeki payda; *M(k)*' nın *LB*' ye yakın olduğu durumlarda benzerliğin daha yüksek olmasını dolayısıyla çözümün iyileşmesini sağlar. Durdurma kriteri, en iyi çözüm üzerinde ilerleme sağlamadan geçen c(õ)Tj / Tr belirli bir nesil sayısıdır. Ayrıca bir zaman sınırı da verilmiştir. Algoritma, 390 örnek problem üzerinde test edilmiştir, her bir işin işlem süresi *[1,k]* aralığında aynı tip dağılımdan seçilmiştir. Algoritma diğer yöntemlere göre daha iyi sonuçlar vermiştir. Özellikle uzun işlem süreli ve az sayıda makinenin olduğu problemlerde algoritma oldukça etkilidir. Yazarlar, iyi performansın nedeninin bağışıklık sisteminin sunduğu yüksek çeşitlilikten kaynaklandığını belirtmişlerdir.

Atölye tipi çizelgeleme problemlerine sağlam çözümler bulmak amacıyla Jensen ve Hansen tarafından bir çalışma yapılmıştır [21]. Gerçek bir sistem için en iyi çizelgeler yerine, değişen şartlara göre üzerinde kolayca değişiklik yapılabilecek çizelgelerin bulunmasının önemine dikkat çeken yazarlar, bu amaca yönelik bir yapay bağışıklık sistemi geliştirmişlerdir. Çalışmada her biri bir miktar genetik dizi içeren kütüphaneler kurulmuştur, her dizi bir atölye tipi problem kümesi çözümünün bir parçasıdır. Atölye tipi probleme çözüm, her kütüphaneden dizileri seçerek (bu dizi bir antikordur) ve seçilen dizinin kodu çözülerek bulunabilir. Her işin başlama tarihleri değiştirilerek bir antijen kümesi elde edilir. Bu antijenler, çeşitli hatalar veya duraksamalar nedeniyle mevcut planlardan farklı olarak ortaya çıkan çizelgelere karşılık gelir. Çalışmada, bir sağlamlık ölçütü tanımlanmıştır. Bu ölçüte göre yapılan değerlendirmeler göstermiştir ki, sağlam çözümler mevcuttur ve bu çözümler YBS ile bulunabilir.

Hart ve diğ., her işin belirli başlama ve bitiş tarihlerinin olduğu atölye tipi çizelgeleme problemlerinde maksimum gecikmeyi, en fazla azaltmak için yapay bağışıklık sistemi modeli kullanmışlardır [22]. Model iki aşamalı çalışmaktadır. Sistemin birinci aşamasında, fabrikada en sık kullanılan ortak iş çizelgeleri modellerini tespit etmek için genetik algoritma ile birleştirilmiş bağışıklık sistemi yaklaşımı kullanılmaktadır. İkinci aşamada, tespit edilen modelleri kullanarak yeni çizelgeler üretmek için doğal bağışıklık sistemlerinin adaptif özellikleri modellenmiştir. Sonuçlar, geniş çaplı bir araştırma prosedürü kullanan bir model ile karşılaştırılmıştır. Önerilen algoritma oldukça başarılı sonuçlar vermiştir, şöyle ki, daha önce ortaya çıkan herhangi bir duruma karşılık gelen çizelgeler kolaylıkla tekrar oluşturulabilmektedir.

Mori ve diğ., bir yarı iletken üretim hattını kontrol etmek için genel bir otonom dağıtılmış sistem tanımlamışlardır [23]. Çalışmalarında, üretim hattının kontrolü bir ajanlar kümesi (detektör, arabulucu, katalizör ve onarım ajanları) ile yapılmaktadır. Her bir ajan üretim hattı ve diğer ajanlarla ilişki içindedir. Bu ilişki omurgalı bağışıklık sistemindeki ilişkiye dayanmaktadır. Örneğin, detektör ajanlar, bağışıklık sistemindeki B hücrelerine karşılık gelir ve sistemdeki belirli aksaklıkları tespit etmek için kullanılır. Sistem pratikte denenmemesine

rağmen, çalışmada sistemin gerçek zamanlı karar vermede ve değişen çevreye uyum sağlamada başarılı olacağı iddia edilmiştir.

**2-** Dasgupta, ve Forrest, alet hatası tespiti için bir yapay bağışıklık algoritması geliştirmişlerdir. Metot; bağışıklık sisteminin öz ve öz olmayan hücreleri birbirinden ayırmayı sağlayan negatif seçim mekanizmasından ilham almıştır [24]. Bu uygulamada 'öz', normal kesme operasyonu değerlerini, "öz olmayan" ise izin verilen kesme kuvveti farklılığının ötesinde herhangi bir sapmayı belirtir. Önerilen algoritma, torna operasyonları için bir simülasyon çalışması ile gösterilmiş ve kalem ucunun bozulması durumunda algoritmanın bunu tespit etme performansı belirlenmiştir. Algoritma, tüm test durumları için kalem ucundaki bozulmaları tespit etmiştir.

**3-** Lee ve diğ. yapay bağışıklık sistemini dağıtılmış, otonom robot sistemine uygulamışlardır [25]. Her robot; bir "B" hücresi, her bir çevresel durum; bir antijen, bir davranış stratejisi; bir antikor ve bir kontrol parametresi de bir "T" hücresi olarak ele alınmıştır. Sistemin çalışmasında; çevresel durum değiştiğinde her robot uygun bir davranış stratejisi seçer ve onun bu davranış stratejisi iletişim ile diğer robotlar tarafından tetiklenir ve yayılır. Sonuçta en çok kabul gören strateji, kümenin davranış stratejisi olarak belirlenir. T hücre modellemesi kullanılarak, robotun dinamik ortamlara uyum yeteneği geliştirilmiştir.

**4-** Dasgupta ve Forrest, zaman serileri verilerindeki farklılaşmaları tespit etmek üzere bir negatif seçim algoritması önermişlerdir [26]. Zamanla kesme kuvveti değerleri değişmektedir. İzin verilen sapmanın ötesindeki değerler sistemdeki 'öz olmayan' ları belirtmektedir. Sistemin elemanlarını tasvir etmek için bir ikilik "Hamming şekil uzayı" uygulamışlardır. Algılayıcılar ile kodu çözülmüş veri arasındaki algılamanın derecesini belirlemek için bir r-ardışık bit kuralı uygulamışlardır. Yazarlar iki veri seti için sonuçları vermişlerdir. Bir tornalama operasyonunun kesici dinamikleri ve bir sentetik sinyal, eşleştirme fonksiyonu ile seçilen *r*-ardışık bitlerinin sayısının hataların tespitindeki riskin güvenilirliğini etkilediğini göstermişlerdir.

### 3.5. Yapay Bağışıklık Sisteminin Bilgisayar Ağları Üzerine Uygulanma Mimarisi

Ağ trafiği, kablosuz ağdaki her bir bilgisayar üzerinde bulunan detektör kümesi ile görüntülenir. Her bir detektör ikilik dizilerden oluşmaktadır ve saldırı tespit işlemi, detektör dizisi ile bağlantılardan elde edilen veri bloğunun karşılaştırılması ile gerçekleştirilir. Karşılaştırma işlemi parçasal olarak yapılmaktadır ve r-ardışık bit kuralı kullanılır. Önce bir algılayıcılar kümesi oluşturulmakta, sonra normal durumlar oluşturulan algılayıcılar ile karşılaştırılarak izlenmektedir. Eğer iki dizideki ortak ardışık bitlerinin sayısı bir r sayısından büyük veya eşit ise, bir eşleşme olmuş demektir [12].

Detektörlerin yaşam süresi süreklidir ve belirtilen yaşam döngüsü doğal bağışıklık sistemindeki antikor hücrelerin yaşam sürelerine benzemektedir. Örneğin T hücreleri ve B hücreleri doğal bağışıklık sisteminde bu görevleri vardır. Başlangıçta rasgele üretilen bir algılama dizisi ile bir detektör oluşturulur ve zamanın belli bir periyodu boyunca bu dizi olgunlaşmamış durumdadır. Bu olgunlaşma periyodu boyunca detektör tüm oluşan veri blokları ile karşılaştırılır. Eğer detektör herhangi bir veri ile eşleşirse bunların arasındaki eşleşme kadar detektör değişikliğe uğrar. Bu işlemde doğal bağışıklık sistemindeki Timus' daki lenfositlerin negatif seçimine benzemektedir. T ve B lenfositlerinin bağışıklık sisteminde görev yapabilmesi için çeşitli olgunlaşma evrelerini tamamlamaları gerekmektedir. Bu geçen zamandaki işlemlere olgunlaşma adı verilir [14]. Herhangi bir eşleşme dışında olgunlaşma periyodunda detektör hayatta kalırsa bu olgun hale gelir ve gelecek karşılaşmalarda sistem kendi kendine uyarı vermektedir. Bu uyarı kablosuz alan ağlarında normal olmayan bir durum algılanması sonucu oluşur. Olgun hale gelen detektör sürekli olarak sistem üzerinde aktiftir. Daha sonra yeni bir durum oluştuğu takdirde detektör bu yeni oluşan duruma göre değişiklik göstererek sistem üzerindeki etkisine devam etmektedir.

Negatif seçim işlemi sistemin geleceği için çok önemli bir rol oynamaktadır. Önemli olmasının sebebi kendiliğinden algılama işleminin gerçekleşmesi için buna ihtiyaç duyulmasıdır. Negatif seçim işlemi tarafından sistemde bir durum bir kez algılandığında, her bir detektör aynı özellikleri taşıyan başka bir durumla karşılaştığı zaman bu duruma karşı bir tepki gösterir. Çünkü sistem aynı özellikleri taşıyan duruma daha önce bir bağışıklık göstermiş ve bu durumu tanımıştır. Doğal bağışıklık sisteminde de bu şekilde bir algılama mekanizması çalışmaktadır. Vücudun karşılaştığı tanınmayan bir antijen saldırısına karşı doğal bağışıklık sistemi organları bu durumu tespit ederek buna karşı bir önlem almaktadır. Aldığı bu önlemi hafıza hücrelerine kaydederek daha sonra oluşabilecek durumlara karşı bir önlem almaktadır. Buda bağışıklık sisteminin en önemli özelliğidir.

# 4. KABLOLU AĞLAR, KABLOSUZ AĞLAR ve GÜVENLİK UNSURLARI

## 4.1. Kablosuz Yerel Alan Ağı Standartları

Kablosuz ağ standartları IEEE 802 çalışma grubu tarafından belirlenmiştir. 802.11 standartları günümüzde oldukça gelişmiştir. Yüksek bant genişlikleri elde edebilmek için geliştirilen standartlar internet ortamındaki veri boyutlarının büyümesiyle orantılı olarak gelişmektedir. Günümüzde kablosuz ağlarda kullanılan standartlar 802.11b, 802.11a, 802.11g, 802.11b+, 802.11i olarak sıralanmaktadır. Standartların gelişmesindeki en önemli etkenlerden biriside güvenliktir. Kablosuz ağların artması beraberinde önemli güvenlik sorunları ortaya çıkarmıştır. Fakat standartların gelişmesi bu güvenlik problemlerini ortadan kaldırmak için yeterli olmamaktadır. Kablosuz ağlar, kablolu ağların birtakım fiziksel problemlerini ortadan kaldırmakta ve ağa dahil olmak isteyen hareketli cihazların kolayca bağlanabilmesini sağlamaktadır. Fakat iletişim radyo dalgaları aracılığıyla korumasız hava ortamında gerçekleştiği için, paylaşılan verilerin güvenliği çok önemli bir konuma gelmiştir. Kablosuz ağlarda güvenliğin çok da iyi olmadığı görülünce de çeşitli önlemler alınmıştır. Bu önlemler erişim noktalarına entegre edilen güvenlik protokolleri olmuştur [27, 28].

### 4.1.1. Kablosuz Yerel Alan Ağı Nedir?

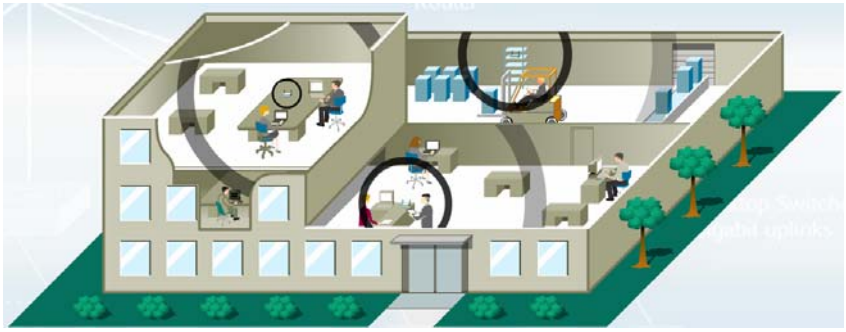
Kablosuz yerel alan ağları, iki yönlü geniş bant veri iletişimi sağlayan, iletim ortamı olarak fiber optik veya bakır kablo yerine telsiz frekansı veya kızılötesi ışınları kullanan ve salon, bina veya yerleşke gibi sınırlı bir alanda çalışan iletişim ağlarıdır . Kurulum kolaylığı ve hareket serbestliği gibi önemli avantajlar sağlayan WLAN sistemleri kablolu ağların yerini alabilmekte ve hatta bu ağlara göre daha fazla fonksiyonlar içerebilmektedir. Kablosuz Yerel Alan Ağları Avrupa düzenlemelerinde Telsiz Yerel Alan Ağları, Radio Local Area Network, Radio LAN, RLAN olarak adlandırılmasına karşın başta ABD olmak üzere birçok ülkede Wi-Fi, Wireless Local Area Networks, Wireless LAN, WLAN olarak adlandırılmaktadır [29].

WLAN sistemleri başlangıçta mevcut kablolu ağların tamamlayıcısı olarak tasarlanmışlardır. Ancak son yıllarda yaşanan teknolojik gelişmeler WLAN sistemlerinin kablolu ağların yerini alabileceğini göstermiştir. Ayrıca mevcut ağların genişleme ihtiyacını karşılamak üzere de WLAN sistemleri yaygın olarak kullanılmaktadır. Kablosuz alan ağı sistemleri başarılı performansları ve düşük maliyetleri ile hem iş çevrelerinde hem de bireysel kullanıcılar arasında yaygın olarak kullanılmaktadırlar. Kablosuz alan ağı kullanıcısı pahalı bir kablolama alt yapısı yerine özünde küçük bir radyo vericisi olan erişim noktası ile iletişim ortamı sağlayabilmekte ve yerel alan ağı oluşturabilmektedir [30]. Temel olarak WLAN sistemi iki ana unsurdan oluşmaktadır. Birincisi AP, ikincisi ise kablosuz cihazlardır. Ancak cihazdan

cihaza (peer to peer) çalışma modelinde AP' ye ihtiyaç duyulmaz. Bu durumda kablosuz ağ kartına sahip bilgisayarlar kendi aralarında ilave bir cihaz veya kabloya ihtiyaç olmadan bir ağ oluşturabilirler. Kablosuz cihazlar genellikle bir dizüstü bilgisayar, kişisel bilgisayar (PC), cep bilgisayarı (PDA), veya kablosuz ağ ünitesi (NIC) ile donatılmış benzeri bir cihaz olabilir. NIC' ler RF veya kızılötesi kullanarak takılı bulunduğu cihaz ile AP arasındaki bağlantıyı sağlar. AP' ler ihtiyaca göre bir eve, iş yerine, toplantı salonuna veya bir binaya kurulabilir. Halka açık kullanımı sağlamak üzere ise şehir merkezlerine, büyük alışveriş merkezlerine, hava alanı, tren istasyonu, otobüs terminali veya restoran gibi kamuya açık alanlara AP kurulabilir. Bu durumda AP' nin oluşturduğu kablosuz internet bağlantısı sağlanan fiziksel alan erişim alanı olarak adlandırılmaktadır. Kablosuz cihazlarda bulunan ara yüz kartları otomatik frekans tarama özelliğine sahip olduklarından kendilerine ulaşan WLAN sinyalini algılayabilirler. Ara yüz kartı tarafından doğru frekans kanalı bulunduktan sonra AP ile kablosuz cihazlar arasında bağlantı kurulumu başlatılır [31].

WLAN sistemleri aslında tamamen kablosuz değildir. Çünkü sistemde bulunan AP' nin geniş bant erişim hizmeti veren DSL, Fiber Optik veya benzeri bir kablolu altyapısı üzerinden şebekeye bağlanması gerekmektedir. Bu nedenle WLAN sistemleri ile tamamen kablosuz olmaktan ziyade kablolama ihtiyacı en az düzeye indirilmiş olmaktadır. Bu açıdan bakıldığında WLAN sistemlerinin artışı geniş bant erişim hizmetinin artışına bağlıdır, ya da WLAN sistemlerinin artışı geniş bant erişim hizmetinin yaygınlaşmasını desteklemektedir. Ancak cihazdan-cihaza kullanımda herhangi bir kablolamaya ihtiyaç olmadığından tam bir kablosuz ağ kurulumu gerçekleşmektedir. Benzer şekilde şebekeye erişim hizmetinin kablo yerine sabit telsiz erişim veya uydu terminali ile sağlanması durumunda da tam bir kablosuz ağ kurulumu gerçekleşmektedir.

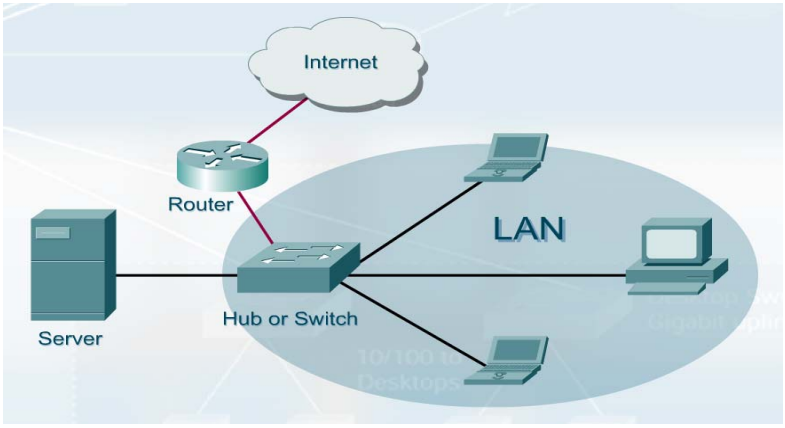
Kablosuz yerel alan ağları token ring ve eternet gibi kablolu ağ teknolojilerinin sağladığı tüm avantajları sağlayabilmektedir.



**Şekil 4.1** Kablosuz Ağ Yapısı

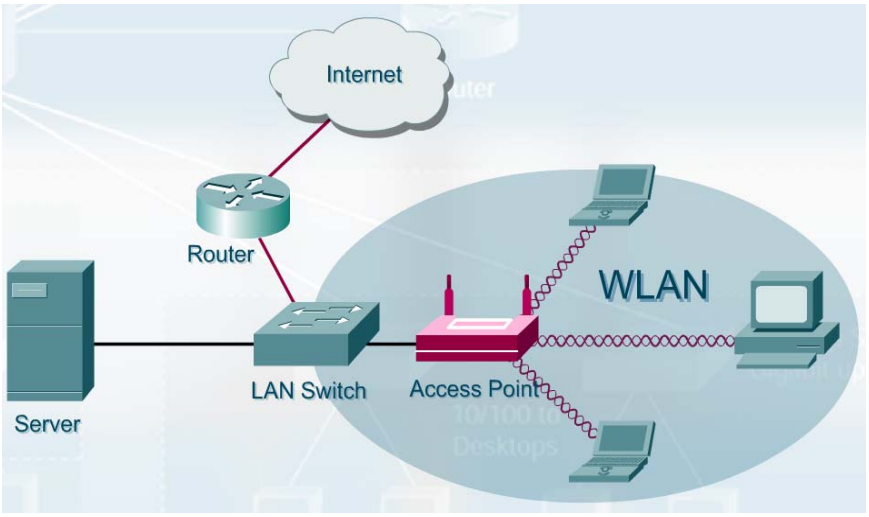
## 4.2. Kablolu ve Kablosuz Yerel Alan Ağları Arasındaki Farklar

Günümüzde kullanılan yerel alan ağlarında masaüstü ya da dizüstü bilgisayarlar genellikle merkezi bir çoğullayıcıya ya da bir anahtar cihazına kablolarla bağlıdır. Bu merkezi noktadan sunucularda bulunan uygulamalara ya da paylaşılmış verilere, internete ise yönlendirici üzerinden erişirler. Bu yerel alan ağların en basit biçimidir [29]. Kablolu yerel alan ağı Şekil 4.2' de gösterilmektedir. Yerel alan ağları bağlantıları kablo üzerinden gerçekleştirmekte ve ağa dahil olan kullanıcılar mutlaka bir kablo ile ağa dahil olmalıdır. Böylece ağa dahil olan kullanıcıları kontrol etmek kolaydır. Sunucudan çıkan sinyal bir çoğullayıcı yada anahtar cihazı gibi ağ cihazları ile kullanıcılara kablo ulaştırılması vasıtası ile ağa dahil olabilmektedir.



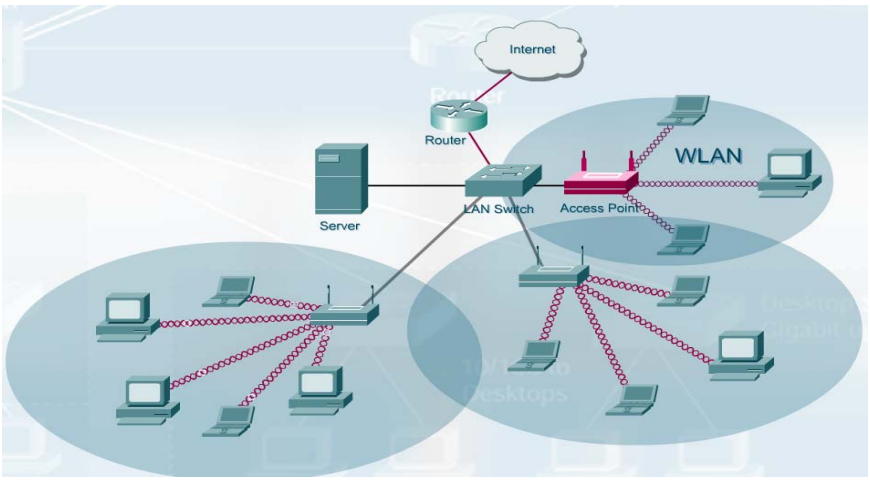

**Şekil 4.2** Yerel Alan Ağı Görünümü

Kablosuz ağlar kablolu ağlara çok benzer olmakla birlikte güvenlik açısından önemli farklar içermektedir. Kablolu ağ mimarisine ek olarak kablosuz ağda merkezi nokta olarak hareket eden erişim noktası eklenmektedir. Erişim noktası aynı zamanda kablolu ağlarla kablosuz ağları birbirine bağlamak için kullanılır. Kablosuz yerel alan ağı yapısı Şekil 4.3' de gösterilmektedir. Erişim noktası kapsama alanı içinde kablosuz istemcilerin trafiğini yönetir ve bu istemcilere radyo sinyalleri yollar. Böylelikle ağa dahil olmak isteyen kullanıcılar radyo sinyallerini çeşitli ağ ara yüz kartları ile alarak kendilerini ağa dahil edebilmektedir. Buda önemli güvenlik problemlerini beraberinde getirmektedir. Erişim noktası kablosuz yerel ağ ve kablolu yerel ağ arasında bilgi alınması gönderilmesi ve ön belleklenmesi görevlerini yerine getirmektedir. Tek bir erişim noktası bağlantı hızına göre birkaç metreden yüz metreye kadar olan bir alan içinde küçük bir kullanıcı grubunu desteklemektedir [28, 29].




**Şekil 4.3** Kablosuz Yerel Alan Ağı Yapısı

Fakat kablosuz bağlanılabilirlik özellikleri arttırılarak bu alan büyütülebilmektedir. Son kullanıcılar kablosuz yerel ağlara bir adaptör kart ile bağlanmaktadır. Adaptör kartlar avuç içi ve diz üstü bilgisayarlarda olabildiği gibi masaüstü bilgisayarlarda da kullanılabilir. Çoklu bağlantılı bir ağ yapısı Şekil 4.4' de gösterilmektedir.




**Şekil 4.4** Çoklu Bağlantılı Ağ Yapısı

## 4.3. Kablosuz Ağlar ile Kablolu Ağlarda Güvenlik Unsurları

Kablosuz ağlardaki en temel güvenlik problemi verilerin havadan yayılan radyo sinyalleri ile iletilmesidir. Kablolu ağlarda anahtar cihazı ya da çoğullayıcı kullanarak fiziksel güvenlik önlemleri alınabilmektedir. Anahtar cihazına ya da çoğullayıcıya fiziksel olarak bağlı olmayan kullanıcılar ağı tehdit edebilecek unsurlar olarak görülmemektedir. Oysa kablosuz

ağlarda tüm iletişim hava ortamı üzerinden yapılmakta ve ağ içerisindeki tüm veriler havadaki radyo dalgalarının üzerinden taşınmaktadır. Kablolu bir ağda oluşabilecek herhangi bir güvenlik probleminde ağa bağlı olan tüm kullanıcılar tespit edilebilmektedir. Fakat kablosuz ağlarda ağa dahil olan kullanıcının tespiti daha karmaşık bir işlemdir. Bu nedenle kablosuz ağlarda oluşabilecek güvenlik tehditlerine karşı geliştirilecek bir tespit sistemi ağı izinsiz kullanan yada istenmeyen ağ durumlarına yol açan kullanıcıları tespit etmekte başarılı olmalıdır. Ayrıca değişen ağ aktivitelerine karşı sistem kendini adapte edebilmeli ve tehdit unsurlarını ortadan kaldırmalıdır. YBS kullanan bir sistem istenen özellikleri sağlamadan başarılar göstermiştir.

# 5. AĞ GÜVENLİĞİ SALDIRI TESPİT SİSTEMLERİ

Kablolu ve kablosuz ağlarda istenmeyen durumların tespiti için birçok saldırı tespit sistemi önerilmiştir [32]. İstenmeyen durumların tespitinde kullanılan sistemlere saldırı tespit sistemi denir. Saldırı tespit sistemlerinin sayıları uygulama yöntemlerine ve uygulandıkları ortama göre çeşitli sınıflara ayrılmaktadır. STS' ler değişik yaklaşımlar ile sınıflandırılabilirler. Bunlar sistemin gerçek zamanlı olup olmaması, dağıtık mimaride olup olmaması, ağ veya sunucu tabanlı olması ve kullandığı analiz yöntemlerine göre sınıflandırmayı içerir. Saldırı tespiti ile ilgili yapılan çalışmalarda farklı tipte saldırı tespit sistem yöntemleri ortaya çıkmaktadır [32].

## 5.1. Saldırı Tespit Sistemlerinin Sınıflandırılması

- **Veri İşleme Zamanına Göre:** Saldırı tespit sistemleri "gerçek zamanlı" ve "gerçek zamanlı olmayan" şeklinde ikiye ayrılırlar. Gerçek zamanlı olmayan sistemlerde veri önce depolanır, sonra analiz için ilgili saldırı tespit sistemine gönderilir. Gerçek zamanlı sistemlerde veri o anda analiz edilir. Bu tip STS yoğun bilgi akışı olan ağlarda uygulanması zor olan ama aktif olarak cevap üretilmesi gereken durumlarda da tek çözüm olan sistemlerdir. Uygulamaların gerçek zamanlı olması tercih edilir. Gerçekleştirdiğimiz uygulamada gerçek zamanlı veriler üzerinde analiz yapılmıştır.
- **Mimari Yapıya Göre:** STS ağ üzerinden birçok noktadan veri toplayıp bir merkezde işleyebilirler. Bu tip mimarilere sahip saldırı tespit sistemlerine dağıtık saldırı tespit sistemleri adı verilir [33]. Bunun karşısında ağ üzerinden tek bir yerden veri toplayan saldırı tespit sistemleri vardır. Bilinen STS 'lerin çoğu bu kategoriye girer. Tezde tek bir yerden veri toplanıp işlenmesi durumu göz önüne alınmaktadır. Bunun için Linux üzerinden ağ trafiğini dinlemeyi sağlayan "TcpDump sniffer" programı kullanılmıştır.
- **Bilgi Kaynaklarına Göre:** STS' ler bilgi kaynaklarına göre ikiye ayrılırlar. Bunlar ağ tabanlı STS' ler ve sunucu-tabanlı STS' lerdir [33]. Sunucu temelli STS' lerin özel bir hali olarak uygulama temelli STS' ler de mevcuttur. Ağ-Temelli STS' lerin temel amacı ağ üzerinden yapılan saldırıları ağ trafiğini gözetleyerek tespit etmektir. Ağ paketlerini yakalayıp bunları analiz ederek saldırı tespiti yaparlar. Son yıllarda geliştirilen ağ temelli STS' ler sunulan çalışmanın da temelini oluşturmaktadır.
- **Sunucu-Temelli STS' ler:** Sunucu-temelli STS' ler bir bilgisayar sistemi içerisinde toplanan veriler üzerinde çalışırlar. Bu şekilde işletim sistemine yönelen saldırılar için hangi sistem çağrılarının ve hangi kullanıcıların sorumlu olduğu tespit edilebilir.

Sunucu-temelli STS' ler iki tür bilgi kaynağı kullanırlar. Bunlar işletim sistemi izleme seçenekleri ve sistem günlük dosyalarıdır. Ağ temelli sistemlere göre bir avantajı, olayların olduğu yerel sunucuyu izleme yetenekleri sayesinde ağ-temelli STS' lerin yakalayamayacağı saldırıları tespit edebilirler. Bu saldırılar çoğu zaman fazla trafik yaratmayan R2L veya U2R saldırılarını içerir.

- **Uygulama-Temelli STS' ler:** Bu STS' ler bir yazılım uygulaması ile meydana gelen olayları analiz eden sunucu-temelli STS' lerin özel bir türüdür [34]. Uygulama-temelli STS' lerde bilgi kaynağı olarak genellikle uygulamaya ait günlük dosyalar kullanılır. Analiz motoruna belirli uygulamalar için o uygulamalara has özellikler bildirildiği takdirde, yetkisini aşan kullanıcıların gerçekleştirdiği saldırılar uygulama-temelli STS' lerce tespit edilebilir.
- **Saldırı Tespit Yöntemlerine Göre:** STS' ler saldırı tespit yöntemlerine göre sınıflandırılırsa iki temel yöntem söz konusudur. Bunlardan birincisi anormallik tespitine dayanır. Diğeri kötüye kullanım tespiti ya da bazı kaynaklarda tanımlandığı üzere imza-tanıma üzerinden gider [34, 35]. Aşağıda iki yaklaşım da ayrıntılı olarak incelenecektir.

### 5.1.1. Anormallik Tespiti

Anormallik (anomaly) normal davranıştan sapma anlamına gelir. Burada normal davranıştan farklılık gösteren davranışların saldırı olarak işaretlenmesi söz konusudur. Normal bir sistemde kullanıcı istekleri tahmin edilebilir istatistiksel değerlerle uyuşur. Normal davranışın bilinmesi ve modellenmesi esastır. Ancak bundan sonra bir anormallik varsa, tespit edilebilir. Belirli kurallar zinciri ile tanımlanabilir veya başka yöntemler uygulanabilir. Fakat sonuçta bu tanımlı ya da öğrenilen davranıştan sapma anormallik olarak değerlendirilerek sapmanın şiddetine göre saldırı olarak sınıflandırılabilir. Bu yöntemin avantajı, daha önceden tanınmayan saldırıların keşfedilmesi olasılığıdır. Dezavantajı ise yanlış alarm sayısının yüksek olmasıdır [36].

Anormallik tespitinde istatistiksel yöntemler, yapay sinir ağları, veri madenciliği yapay bağışıklık sistemi gibi birçok yaklaşım uygulanabilir.

Bunları kendi içinde sınıflandırmak gerekirse:

**Kendi-kendine öğrenen sistemler:** Belli bir veri seti ile eğitilerek normal davranışı öğrenirler. Bunlar, zaman serilerini kullanmayan kural tabanlı sistemler, açıklayıcı istatistikleri kullanan sistemler, zaman serilerini kullanan yapay sinir ağları temelli teknikler ve insan bağışıklık

sisteminden esinlenilerek ortaya çıkmış olan yapay bağışıklık sistemleri olarak gruplandırılmaktadır.

#### 5.1.1.1. Zaman Serisi Kullanmayan Sistemler

- **Kural Tabanlı Sistemler**: Sistem, kendisi trafiği inceleyip kurallar oluşturur ve saldırı tespiti sırasında belirlenen kurallara göre davranıyorsa bu sınıfa girer.
- **Açıklayıcı İstatistikleri Kullanan Sistemler**: Kullanıcı profilinin basit istatistiklerle oluşturulup, buradan uzaklık vektörlerini kullanarak karar alan sistemlerdir.

#### 5.1.1.2. Zaman Serisi Kullanan Sistemler

**a)Yapay Sinir Ağları:** Burada sistem önceden bir zaman serisi ile eğitilir ve çalışmaya başladığında, buradan öğrendikleri ile karar verir.

**b)Yapay Bağışıklık Sistemleri:** Yapay bağışıklık sistemleri insan vücudundaki antikorların mikrop ve mikroorganizmalara karşı vücudu koruması yaklaşımından ortaya çıkmıştır [25]. Sistem rasgele detektörler üreterek ağda oluşan istenmeyen durumları tespit etme ve tekrar aynı durumlarla karşılaşması halinde otomatik yanıt verme yapısına göre çalışır.

**c)Programlanan Sistemler:** Programlanan sistemler kendi içerisinde özelliklerine göre sınıflandırılmaktadır. Bunlar aşağıdaki gibidir.

- **Açıklayıcı İstatistikleri Kullanan Sistemler:** Burada profiller daha önceden tanımlanmıştır. Profilleri sınırlayan belli bir eşik değeri, bir istatistiksel büyüklük veya basit bir kural olabilir. Sistem bu profillere göre istatistik kurarak tespit işlemini gerçekleştirir.
- **Bilinmeyeni Reddet Yaklaşımı:** Tek başına çok sık kullanılmaz. Sistem davranışındaki durum-geçiş değerlerini kontrol ederek, farklı bir geçiş görüldüğünde izin vermemek şeklinde bir yaklaşıma sahiptir.
- **Sinyal İşleme Tekniklerini Kullanan Yaklaşım:** Burada sistem parametreleri sinyal işleme teknikleriyle belirlenir ve saldırı içermeyen normal veri setinden çıkartılan eşik değerleri ile anormallik tespiti yapılır. Bu yaklaşım diğerlerine göre yenidir ve çok geniş bir alanı kapsamaktadır. Henüz sınırlı sayıda sinyal işleme tekniği saldırı içeren zaman serilerine uygulanmıştır. Özellikle son yıllarda popüler olan temel bileşen analizi yaklaşımı ile elde edilen öz değerlerin sistem parametresi olarak kullanılması bu alandaki çalışmalardandır.

#### 5.1.1.3. İmza Tanıma Temelli Saldırı Tespiti

Kötüye kullanım tespiti (Misuse detection) ya da imza tanımaya dayalı sistemlerde ise her davranışın bir imzası vardır. Bunlar daha önce görülen davranış şablonlarıdır. Eğer gözlemlenen davranış daha önceden bilinen bir saldırı imzası ile eşleşiyorsa saldırı olarak sınıflandırılır. Daha önce karşılaşılmadıysa saldırı olarak nitelenmez. Avantajı saldırıyı kesin olarak tanıyabilmesidir. Yani yanlış alarm vermezler. Fakat yeni bir saldırı gelirse bunu sezemezler. İmza temelli sistemler daha çok ticari sistemlerde kullanılırlar. İmza tanımaya dayalı sistemlere ait yaklaşımlar sınıflandırılırsa [37]:

**a) Programlanan Sistemler**: Kendi kendine öğrenen karma bir teknik olan ripper dışında tüm imza temelli teknikler bu sınıfa girerler.
**b) Durum Modellemesi:** Burada tüm davranışlar durumlara karşı düşer. Eğer bir davranış daha önceden tanımlı durumlara ve durum geçişlerine denk düşen hareketler yapıyorsa saldırı olarak tanınır.
**c) Uzman Sistemler:** Sızma belirleme sistemlerin ilkleri kural-tabanlı uzman sistemlerdir.
**d) Örüntü Eşleme:** Sistemde daha önceden tanımlanmış, olmaması gereken bazı sözcüklerin tanınmasına yardım eder. Esnek değildir fakat basittir. Örneğin "parola dosyasını kopyala" komutu görüldüğünde bunun bir saldırı olduğunu en basit şekilde bu yöntem tespit eder.

Saldırı tespit sistemlerinin çeşitliği uygulama katmanının önemini ortaya çıkarmaktadır. Uygulamada kullanılacak yapıya uygun bir saldırı tespit yöntemi seçilmelidir. Çalışmada saldırı tespit yöntemlerinden YBS kullanılmış ve gerçek zamanlı uygulamalar gerçekleştirilmiştir.

### 5.2. Kablosuz Alan Ağları ile Kablolu Alan Ağlarında Saldırı Tespit Sistemi Farkları

Saldırı tespit sistemleri uygulandıkları ağ sistemlerine birçok farklılıklar içermektedir. Kablolu ağlar üzerine uygulanan saldırı tespit sistemleri ağ kullanıcıları üzerinden paket trafik kontrolü yaparak saldırıları tespit mekanizmasına göre çalışmaktadır. Bu şekilde uygulanan bir saldırı tespit sisteminde ağ trafiğini izlemek bütün durumlarda mümkün değildir. Oluşturulan yerel alan ağı bir anahtar cihazı üzerinden dağıtılıyorsa bu durumda ağ trafiğinin tümünü herhangi bir kullanıcı üzerinden izlemek mümkün değildir. Anahtar cihazına bağlı bir kullanıcı sadece kendine gelen giden TCP paketlerini görebilmektedir. Oysa tüm ağı etkileyebilecek bir saldırı durumunda tespit sistemi istenmeyen durumları algılamada hatalar verecektir. Böyle sistemler için her kullanıcı üzerinden ayrı ayrı saldırı tespit programları çalıştırılarak her bilgisayar için ayrı tespit işlemi gerçekleştirilir [12]. Yapay bağışıklık sistemi ile yapılan böyle

bir saldırı tespit sistemi virüs yazılımları gibi benzeri yazılımlardan tek fark olarak bağışıklık mekanizmasına sahip olarak çalışacaktır. Oysa kablosuz alan ağlarında radyo sinyallerini yayan erişim noktaları paketleri tüm ağa ulaştırabilmekte ve ağa dahil olan herhangi bir kullanıcı ağı tehlikeye sokabilmektedir. Erişim noktası yaydığı radyo sinyalleri ile tehlikeye açık bir sistem yaratmaktadır. Bu özellikten faydalanmak istenen kötü niyetli kullanıcılar radyo sinyallerini alarak ağa dahil olup ağ trafiğini dinleyebilmektedir. Buda önemli güvenlik sorunlarını ortaya çıkarmaktadır. Böyle bir ağ üzerine kurulacak olan saldırı tespit sistemi tüm ağı kontrol altında tutabilme özelliğine sahip olmalıdır. Yapay bağışıklık sisteminin istenmeyen durumları tespit etme özelliğinden faydalanarak böyle bir ağda tüm ağa radyo dalgalarını yayan erişim noktası üzerinden yapılacak saldırı tespiti ile tüm ağ istenmeyen durumlardan korunabilmektedir. Gerçekleştirdiğimiz sistem böyle bir ağda oluşabilecek istenmeyen ve tehlikeli durumlara karşı erişim noktasından gözlem yaparak engelleme özelliğine sahiptir.

# 6. KABLOSUZ AĞLARDA SALDIRI TESPİTİ İÇİN YAPAY BAĞIŞIKLIK MODELİ

## 6.1. Genel Bilgi

Saldırı tespiti için bir yapay bağışıklık modeli kullanılabilir. Daha önce açıklandığı gibi saldırı tespit sistemlerinin birçok farklı tipi farklı problemlere uygulanmıştır. Saldırı tespiti, insan bağışıklık sistemi ile ilişkilendirilerek çeşitli alanlara uygulanmıştır. Çünkü her iki sistem, saldırı tespit sistemi ve insan bağışıklık sisteminin asıl amacı istenmeyen durumlara karşı kullanıcıları korumaktır. Bu sebeple saldırı tespiti için yapay bağışıklık sistemi uygulamaları artmıştır.

Bununla birlikte, her biri farklı olan YBS uygulamaları tamamen probleme odaklı olarak fayda sağlayacak şekilde birbirinden ayrılmaktadır [21]. Bu farklılıkların sebebi insan bağışıklık sisteminin çok karmaşık bir sistem olması ve tam olarak anlaşılamamasıdır. Her YBS insan bağışıklık sisteminin farklı özerliklerini içermektedir. Sonuçta YBS uygulanırken bağışıklığın çeşitli özellikleri seçilir. Bunun sebebi uygulanacak YBS için bağışıklık sisteminin faydalarına ihtiyaç duyulmasıdır. Seçilen özellikler, YBS de uygulanacağından bağışıklık sisteminin nasıl olduğunu anlamak çok önemlidir. Böylece insan özellikleri yapay bağışıklık sitemleri ile sağlanabilir. Yeni bir YBS modeli oluşturulurken, verilen bir uygulamanın tüm gereksinimlerini sağlanmalıdır. Çalışmada doğal bağışıklık sisteminin negatif seçim özellikleri üzerinde durulmuştur. Bunun sebebi negatif seçimin insan vücudundaki istenmeyen mikroorganizmaları tespit etmekte kullanılmasıdır. Çalışmadaki amaç ağ saldırılarını tespit etmek olduğundan bu odaklanma gerekmiştir.

Mimari oluşturulurken ağ tabanlı STS sistemi seçilmiştir. Çünkü ağ tabanlı STS ile tüm ağ izlenebildiğinden kullanıcı tabanlı olarak da kullanılabilir. Ağ tabanlı STS aslında çoklu kullanıcı tabanlı bir yapıdır. Hedefleri sağlayacak gereksinimleri ve ağ tabanlı saldırı tespiti için gereksinimler bu bölümde bir yapı içerisinde tanımlanacaktır. Analiz hedefimiz, basit bir yöntem ile negatif seçim algoritmasını uygulamak ve detektör kümelerini elde etmektir.

## 6.2. Ağ Tabanlı Saldırı Tespit Sistemi Gereksinimleri

Ağ tabanlı saldırı tespit sistemleri çeşitli gruplar içerisinde gösterilmekle beraber, her bir yaklaşım farklı problemleri beraberinde getirmektedir. Problemleri çözebilecek tam bir ağ tabanlı model yoktur. İnsan bağışıklık sisteminin özellikleri sunulmadan önce yetenekli bir ağ tabanlı saldırı tespiti tasarımı için gerekli fonksiyonların neler olduğu belirlenmelidir. Çalışmada bu özellikler yedi ana başlık altında toplanmıştır [39].

***Sağlamlık:*** Oluşturulan sistem sağlam bir tespit noktasına sahip olmalıdır. Saldırı tespit sistemi üzerinde herhangi bir sistem hatasını ve tekrarlayan ataklara karşı yeterince güçlü olmalıdır [12]. Buradaki kritik nokta, saldırılar tarafından sistem durdurulmamalı ya da çökertilmemelidir.

***Ayarlanabilirlik:*** Her bir kullanıcı yada ağ cihazları yerel gereksinimlere göre kolaylıkla ayarlanabilmelidir [41]. Ağ ortamındaki her bir kullanıcı heterojendir. Bu kullanıcılar farklı güvenlik ihtiyaçları duyabilir. Ağ için ise, örneğin yönlendirici, filtreleme, DNS, güvenlik duvarı veya çeşitli ağ servisleri ihtiyacı olabilir.

***Genişleyebilirlik:*** Sisteme herhangi bir kullanıcı eklendiğinde basit işletim sistemi ayarlarıyla STS bunun kolaylıkla görmek zorundadır [42]. Ağa yeni bir kullanıcı eklendiğinde ve bu kullanıcı farklı bir işletim sistemi kullandığında bunu görmek kolay değildir. Fakat erişim noktasın üzerinde yapılan bir saldırı tespiti ile tüm kullanıcılar görülebilir.

***Ölçeklenebilirlik:*** Dağıtık kullanıcılardan doğru bilgileri alıp analiz yapmak ve gerekli gruplandırmaları yapabilmek için gereklidir. Veri kayıpları dışında basit bir STS analizi için tüm veriyi geri göndermek çok zordur. Eğer tüm bilgi doğru bir şekilde ölçeklense bile ağ performansında sorunlara yol açabilecektir.

***Uyarlanabilirlik:*** Dinamik olarak değişen ağ saldırılarını tespit etmek için dinamik ayarlamalar olmak zorundadır [42]. Bilgisayar ağları statik değildir. Kullanıcılar, sağlayıcılar ve sistem yöneticileri sürekli değişiklikler gösterir. Ayrıca ağın normal çalışması ve saldırılar, bulundukları ortama göre sürekli değişiklik göstermektedir.

***Genel Analiz Edilebilirlik:*** Saldırıları tespit etmek amacıyla çoklu durumlar arasındaki ilişkiyi tanımlamak ve yeterli olan durumları toplamak için çeşitli kullanıcılar üzerinde çoklu durumları bir arada izlemek zorundadır [41]. Ağ saldırıları istismar ettikleri ağın genellikle tüm kullanıcılarını kullanılamaz hale getirmeye çalışır. Fakat bazen ağdaki tek bir kullanıcıda normal ağ durumları gözlenebilir. Bu durum ağda saldırı olmadığını göstermez. Eğer tüm ağ kullanıcıları gözlenirse saldırının nereden kaynaklandığını yada hangi kullanıcıları etkilediği görülebilir. Bu nedenle erişim noktası üzerinden yapılacak saldırı tespiti ile genel analiz yapılabilir.

***Verimlilik:*** Ağ ve kullanıcı sistemleri üzerinden izleme yapılırken basit ve yeterli miktarda düşük ek yükler getirmelidir [41, 12]. Basit bir saldırı tespit sisteminden izleme, veri toplanması

ve karar vermesi için iyi performans beklenir. Doğru tasarlanmayan saldırı tespit sistemleri kullanıcı bilgisayarlarında işlemci ve giriş-çıkış birimleri için ağır performans kayıplarına yol açabilir. Bu nedenle oluşturulacak saldırı tespit sistemi ağ ve ağ cihazlarının performansında büyük kayıplara yol açmamalıdır.

Verimli saldırı tespit sistemi tasarımları için çeşitli yaklaşımlar önerilmişse de kablosuz ağ saldırı tespitleri için tam çözümler bulunamamıştır [40].

## 6.3. Erişim Noktası Tabanlı Saldırı Tespit sisteminin Tasarım Amacı

Tasarımda etkin bir saldırı tespit sistemi için üç temel tasarım hedefi bulunmaktadır. Bunlar dağıtık olarak çalışabilmesi, kendi kendine organize olabilmesi ve düşük maliyetler getirmesidir. Çalışma bu üç temel hedefi elde etmeye yöneliktir.

### 6.3.1. Dağıtıklık

Tasarımdaki ilk hedef dağıtıklıktır. Dağıtık bir erişim noktası tabanlı saldırı tespit sisteminin yetkileri, sistem içerisindeki kullanıcıların sayısından sorumludur. Bağımsız saldırı tespit işlemlerinin her biri, tüm sistemin sadece küçük birer açısını izler. Aynı zamanda çalışırlar ve her biri diğeriyle bir arada devam eder. Erişim noktası tabanlı saldırı tespiti kullanılırsa aşağıda belirtilen ihtiyaçlar karşılanacaktır.

***Sağlamlık:*** Erişim noktası tabanlı saldırı tespiti için bölgesel saldırı tespiti işlemlerinin birinin başarısızlığı tüm STS' yi kesintiye uğratmayacaktır. Tüm sistem için düşünülürse minimum kayıplara yol açacaktır.

***Ayarlanabilirlik:*** Basit bir saldırı tespit işlemi diğer kullanıcıların çeşitli gereksinimlerini içermeksizin özel bir kullanıcının ihtiyaçlarına göre kolayca ayarlanabilir.

***Genişleyebilirlik:*** Farklı bir işletim sistemine sahip bir kullanıcı ağa eklendiği zaman bu yeni bir kullanıcı için yeni bir saldırı tespit işlemi yapılmasına gerek duyulmayacaktır. Çünkü saldırı tespit işlemleri kullanıcıdan bağımsızdır ve sonuçta yeni bir kullanıcı eklendiğinde var olan işlemlerin değiştirilmesine gerek duyulmaz

***Ölçeklenebilirlik:*** Ölçeklenebilir bir saldırı tespit sistemi ağ kullanıcılarının belirli bir bölümünü kontrol edebilmelidir. Elde edilecek veriler çeşitli ihtiyaçlara göre gruplandırılabilir. Çalışmada erişim noktasından yapılan saldırı tespiti ile sistemin tümüne hakim olunabilmektedir. Böylece merkezi noktadan tüm veri istenildiği gibi ölçeklenebilir.

### 6.3.2. Kendi Kendine Organizasyon

YBS' de ikinci hedef kendi kendine organizasyondur. Önceden tanımlanan ağ durumlarına göre saldırı tespiti yapan erişim noktası tabanlı STS, sonradan oluşabilecek farklı saldırı tiplerini öğrenme yeteneğine sahiptir. Bu işlemi sistem içerisinde değişen ağ çevresi, çeşitli güvenlik gereksinimleri ve yeni gelen saldırılar olduğu sürece başarır. Farklı oluşacak durumlara YBS kendi kendini organize edebilecek özelliklere sahiptir. Eğer erişim noktası tabanlı saldırı tespit sistemi kendi kendini organize ederse bu aşağıdaki faydaları sağlar.

***Uyarlanabilirlik:*** Uyarlanabilirliğin yüksek olması mümkündür. Çünkü ağ ortamının değişikliğinde elle bir saldırı tipi değişikliğine ihtiyaç duyulmaz.

***Bütünlük Analizi:*** Tüm saldırı tespit sistemi basit olarak bütünlük analizi sağlar. Çünkü tüm ağ gözlemlenebilmekte ve ağ kullanıcıların tamamı izlenebilmektedir. Böylece, ağ üzerinde oluşabilecek bütün durumların analizi yapılabilir.

### 6.3.3. Düşük Maliyet

Saldırı tespit sistemi, bilgisayar kaynaklarını en düşük düzeyde harcamalıdır. Düşük kaynak tüketimli erişim noktası tabanlı saldırı tespit sistemi CPU ve giriş çıkış birimlerini aşırı yüklememelidir. Çünkü saldırı tespit sistemlerinin asıl amacı saldırıları tespit etmektir. Eğer, ağ ve ağ cihazlarının çalışmasını güçleştirirse saldırı tespitinin amacı kalmamış olur. Erişim noktası tabanlı bir saldırı tespit sistemi düşük kaynak tüketimi olursa aşağıdaki faydaları sağlayacaktır.

***Verimlilik:*** Kullanıcı tabanlı saldırı tespit sistemi uygulamalarında her bir kullanıcı bilgisayarı üzerinde uygulama çalışır. Buda, ağ ve kullanıcıların bilgisayar verimliliklerini düşürür. Erişim noktası üzerinden bir saldırı tespiti gerçekleştirilirse bu verim düşüklülüğü ortadan kalkacaktır.

## 6.4. Erişim Noktası Tabanlı Saldırı Tespiti için İnsan Bağışıklık Sisteminin Özellikleri

Başarılı bir analiz yapabilmek için insan bağışıklık sisteminin karmaşık yapısının özellikleri iyi analiz edilmelidir. Bu erişim noktası tabanlı saldırı tespiti için birkaç önemli karakteristiğin tanımlanması ile mümkündür. Çalışmada elde etmeyi hedeflediğimiz üç amaç olan dağıtıklık, kendi kendine organizasyon ve düşük kaynak harcaması, erişim noktası tabanlı saldırı tespit sistemi öğelerinin özellikleri ile açıkça belirlenmiştir.

### 6.4.1. Dağıtık Model

İnsan bağışıklık sistemi dağıtıktır. Bu işlemi tamamen dağıtık şekilde antijenleri tespit etmek için insan bağışıklık sistemi mekanizması sağlar.

***Bağışık Ağ:*** İnsan bağışıklık sistemi, farklı tipte hücrelerin büyük bir miktarı arasındaki ilişkilerin tamamını gerçekleştirir. Merkezi koordinatörün çalışması dışında insan bağışıklık sistemi antijen kullanan aktivasyonlar ve antijen yok etme arasındaki denge durumun koruyarak bağışıklık cevabını sağlar.

***Tekil Antijen Kümeleri:*** İnsan bağışıklık sistemi, farklı antijenleri tespit etmek için çeşitli antikor grupları üretir. Bu evrim mekanizması, detektör kümelerinin doğal seçimi boyunca ve farklı antikor kümeleri ile elde eder. Her bir antikor kümesi, tek ve bağımsızdır. Bu özelliklere herhangi bir merkezi yönetime gerek duymaz ve yerel antikor seviyesinde antijenleri tespit etmek için insan bağışıklık sistemine izin verir [42].

### 6.4.2. Kendi Kendine Organizasyon

Kullanılan bağışıklık sistemi yapısı, iki evrim sürecinden oluşur. Bunlar, etkin detektör kümelerinin oluşması ve antikorların elimine edilerek yaklaştırıldığı negatif seçim aşamalarıdır. Bu iki süreç önceden hazırlanan bilgiler veya merkezi erişim noktasındaki uygulama tarafından doğrudan kendi kendine organize olur

***Detektör Kümelerinin Oluşumu:*** Antikorlar, sadece antijenleri değil kendi hücrelerinin özelliklerini de bütünler ve tanır. Bazı bilinen antijen özellikleri yetenekli antikorların üretimi için gereklidir. İnsan bağışıklık sistemi, belirli evrim süreleri ile öğrenir ve bunu bilinen zengin DNA yapısı ve etkinliği ile kendi sağlar. Kendi kendine organizasyon işleminden dolayı detektör kümesine gözlemlenen antijenlerin özellikleri kaydedilir ve ikincil saldırı tespitinde bu detektör kümeleri kullanılır.

***Negatif Seçim:*** İkinci süreç negatif seçim sürecidir. Uygun olmayan ve olgunlaşmamış antikorlar elimine edilir. Bağışıklık sisteminin en önemli özelliklerinden biri kendi hücrelerini saldırı olarak görmemesidir [14]. Kendi hücreleri hakkında herhangi bir bilgiye sahip olması, timusta ve kemik iliğinde gerçekleştirilir.

### 6.4.3. Düşük Maliyet

İnsan bağışıklık sistemi düşük bir maliyetle gerekli işlemleri gerçekleştirir. Uygulamada insan bağışıklık sisteminin düşük kaynak harcamasını nasıl sağladığını anlayabilmek için üç soru üzerinde durulmuştur. Bunlar;

**1**-Nasıl çok miktarda antijen az miktarda antikor ile tespit edilebilir?

**2**-Nasıl antijen bilgileri verimli olarak yeniden kullanılabilir?

**3**-Nasıl birçok antikor sınırlı sayıda detektör ile elde edilebilir?

Bu soruların cevabını bağışıklık sistemi ve bağışıklık sisteminde bulunan hafıza hücreleri ve negatif seçim işlemleri vermektedir.

## 6.5. Kablosuz Ağ Saldırı Tespiti için Yapay Bağışıklık Sistemi Modeli

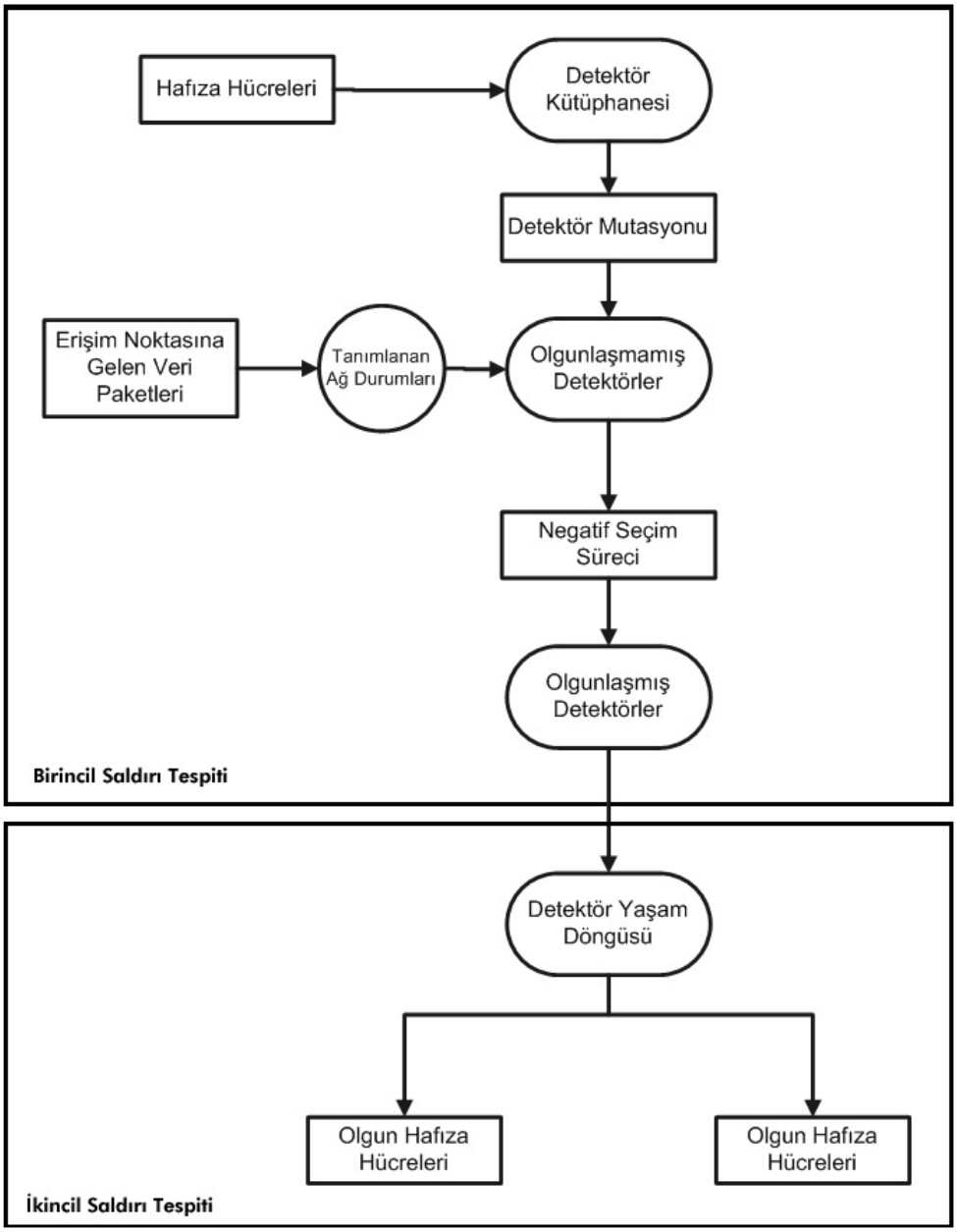
### 6.5.1. Genel Bilgi

İnsan bağışıklık sistemi vücudu farklı tipte patojen ve organizmalara karşı başarılı bir şekilde korumaktadır. Bu olağanüstü özellik bilgisayar güvenliği ile ilgilenen araştırmacıların ve yapay zeka araştırmacılarının ilgisini çekmiştir. Bağışıklıkla uğraşan çalışmacıların, çalışmalarının temelinde bilgisayar sistemleri için farklı bilgisayar bağışıklık modelleri bulunmaktır. Bu modellerin ana fikri normal durumlar (öz) ile normal olmayan durumların (öz olmayan) ayırt etmektir. Bu işlem gözlemlenen ağın normal davranışlarına öz diğer tanınmayan ağ aktivitelerini öz olmayan olarak ayırmaktadır. Birçok ağ saldırıları sweep, koordinat ataklar ve internet solucanları ağ trafiğinde anormal olarak tespit edilir. Birçok ağ tabanlı saldırı tespit sistemi ağ paketlerin izler ve bu ağ saldırılarının kritik imzalarının görerek anormal olarak tanımlar. Sonuçta yapay bağışık sistemi modeli normal ağ aktiviteleri ile anormal network aktivitelerini birbirinden ayırt etmek için tasarlanır ve çeşitli ağ saldırılarını tespit etmesi beklenir.

İnsan bağışıklık sistemi için kemik iliği ve timus çeşitli detektör hücrelerini sürekli olarak üretir ve ikincil lenfosit düğümlerine dağıtır. Detektör hücreleri yaşayan hücreleri gözlemek için vücuda yerleşirler ve ikincil lenfosit düğümleri içerisinde tanınmayan hücreleri tespit eder. Yapay bağışıklık modeli için bu ilk saldırı tespit sistemidir. Oluşturulan mimari Şekil 6.1 de gösterilmektedir. Tüm paket trafiği erişim noktasından alınmaktadır. Oluşturulacak her bir detektör bireyi kablosuz ağın anormal durumlarını tanımalıdır. Bu detektörler tektir. İkincil saldırı tespitinde önceden saldırı olarak tanımlanan detektörler cevap verir buna ikincil bağışıklık adı verilir. İlk bağışıklıktan sonra hafızaya alınan detektörler ikincil bağışıklık yanıtını verir.

Tasarlanan mimari ile bölüm 6.3’ de verilen üç temel hedefi sağlayacak bir saldırı tespiti oluşturulmuştur. Dağıtıklık, kendi kendine organize olabilme ve düşük maliyet ile

koruma yapma yeteneklerine sahiptir. Mevcut bilgisayar bağışıklık modelleri tek kullanıcının kullanabileceği yapılar üzerine odaklanmıştır. Oluşturulan mimari ile tek kullanıcı yerine erişim noktası tabanlı bir sistem önerilmiş ve bir saldırı tespit sisteminden elde edilmesi gereken faydalar elde edilmiştir. Şekil 6.1' de ilk aşamada detektörler oluşturulmakta bu işlem yapılırken negatif seçim algoritması kullanılmıştır. Oluşturulan detektörler tanımlanan normal ağ çalışmasından farklı olan durumlara göre oluşturulur. İkinci aşamada, ikincil saldırı tespiti için hafıza hücreleri kullanılmıştır. Bu aşamada, hafıza hücrelerine dönüşecek olgun hafıza hücreleri detektörlerin yaşam döngüsü içerisinden elde edilmektedir. Tüm paketler kullanıcılardan gelip erişim noktasına ulaşmakta ve buradan sistemdeki çevrime katılmaktadır. Sistem başlangıçta korunması gereken ağ durumlarını kullanarak detektör kümeleri oluşturur. Detektör kümeleri oluşumunu negatif seçim algoritması ile gerçekleştirir. Negatif seçim mevcut durumlarla rasgele durumların karşılaştırılması sonucu tanınmayan durumları tespit edebilecek detektör kümeleri oluşturur. Yaşam döngüsünden çıkan ve sistem içerisinde kullanılan detektörler detektör kütüphanesine kaydedilir. Tanınmayan durumları tespit etme yeteneğine sahip olan detektörler bu kütüphaneye kaydedilir.




**Şekil 6.1** Erişim Noktası Tabanlı Yapay Bağışıklık Modeli

### 6.5.2. Birincil Saldırı Tespiti

Birincil saldırı tespiti negatif seçim işlemi temeline göre oluşturulur. Negatif seçim sürecinde farklı detektörlerin üretilmesi amaçlanır. Farklı detektörler ağın normal tanınan durumlarıyla eşleşmez ise detektör kümesine kaydedilirler. Yapay bağışıklık sisteminin detektör kütüphaneleri potansiyel etkin olabilecek detektörleri depolar, etkin detektörler ikincil saldırı tespiti için saklanır, sonuçta detektör kütüphanelerinde anormal ağ durumlarını tespit etmek için detektörler toplanır. Bu detektörler, yeni detektörler oluşturmak için mutasyon işlemine tabi

tutulabilir. Detektör kütüphanelerindeki detektörler, daha sonraki durumlarda normal ağ paketlerini anormal olarak algılayabilir. Bu durumda detektör kütüphaneden silinir. Bu mekanizma, yapay bağışıklık sisteminin hafıza aşaması olup bu özellik kendi kendine organize olma özelliğidir ve çok düşük maliyetleri vardır.

Erişim noktasından yapılan bir saldırı tespiti ile tüm ağ için belirli sayıda detektör kullanımı söz konusudur. Eğer, tüm kullanıcılarda uygulama çalıştırılırsa her kullanıcı için farklı detektör setleri oluşturmak gerekecektir. Erişim noktasındaki tek detektör kümesi ile tüm ağın kontrolü yapılabilir. Böylece, ağ ve ağ cihazlarının performans maliyeti yani kaynak harcaması düşürülebilir.

Normal ağ durumları kümesi rasgele üretilen olgunlaşmamış detektörlerin eşleşmesi için başlangıçta tanımlanmıştır. Diğer bir değişle, bu durumlar gözlemlenen normal ve anormal ağ davranışlarını belirler. Bununla birlikte bazı olgunlaşmamış detektörler hatalı detektörler olabilir. Bu hatalı olgunlaşmamış detektörler negatif seçim işlemi süresince silinir. Olgunlaşmamış detektörler ile tanınan durumlar arasında eşleşme uygunsa ve önceden tanımlanan eşik değerinin üzerindeyse bu yeni olgunlaşmamış detektörler yanlış detektörler olarak belirlenir. Yaşam döngüsü içerisinde bulunan detektörler önceden belirlene tolerizasyon periyodu boyunca kontrol edilir. Tolerizasyon periyodu detektörlerin minimum eşleşme süreleridir. Eğer tolerizasyon periyodu süresince detektör ağ durumlarıyla eşleşmezse detektör silinir. Bu detektörler normal aktiviteleri anormal olarak hatalı tespit yapabilir. Sonuçta bu kendi kendine organizasyonun özelliklerini gösterir.

Son aşamada negatif seçimden hayatta kalan detektörler bir yaşam döngüsü içerisine girerek olgun detektörlere ve hafıza hücrelerine dönüştürülür. Bu detektör seti yerel kullanıcılardan gelen verilerin içerisinde ağ saldırılarını tespit ederek yapay bağışıklık sisteminin dağıtık özeliklerini sağlar. Seçilen detektör kümesi ve normal ağ trafik davranışları ikincil saldırı tespiti cevabında kullanılmak üzere erişim noktasına aktarılır. Bu sürecin performanslı olması için birincil saldırı tespit sistemi ikincil saldırı tespit sistemi ile iletişim halinde olmalıdır. Buradaki hafıza birimi birincil saldırı tespiti ile ikincil saldırı tespiti arasında ilişkiyi kurmayı sağlar.

### 6.5.3. İkincil Saldırı Tespit Sistemi

İkincil saldırı tespit sistemi evrim sürecinin son aşamasıdır. Burada detektörler bir yaşam döngüsü içerisine girer. Bu aşamada olgunlaşmamış detektörler olgunlaşmış detektörlere dönüştürülerek hafıza hücrelerinde saklanacak hale getirilir. Bu görevler farklı birkaç bileşenin operasyonu ile elde edilir. Bileşenler tanınan ağ durumları, negatif seçim, ağ trafiği anormal tespiti, hafıza hücreleridir. Anormal bir durum tespit edildikten sonra ikincil saldırı tespit

sistemi devreye girer. Yeni bir detektör anormal bir ağ trafik aktivitesi tespit ettiği zaman bu detektör ikincil saldırı tespiti için hafıza hücrelerine kaydedilir. Böylece gelecekte oluşabilecek benzer saldırılar hızlı bir şekilde tespit edilir. Ayrıca bu detektörler birincil saldırı tespitinde detektör kütüphanesinde bulunmuyorsa eklenir. Hafıza hücrelerine kayıt işlemi yeni durumların tespit edilmesinde düşük performans harcamaya sebep olacaktır. Buda modeli düşük maliyetli yapmaya yardımcı olmuştur.

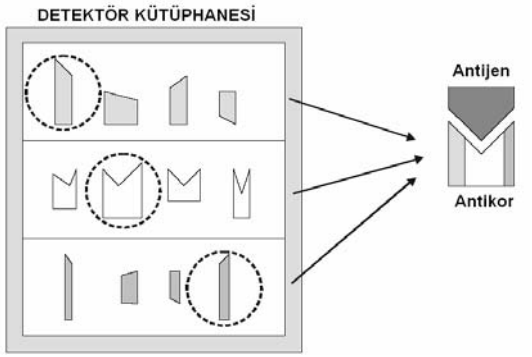
## 6.6. Kullanılan Negatif Seçim Algoritması

Erişim noktası tabanlı saldırı tespiti için ayrıntılı yapay bağışıklık modeli önceki bölümde anlatılmıştır ve iki farklı evrim süreci içermektedir. Bunlar negatif seçim ve hafıza hücrelerinin oluşumudur. Bu model, ağ saldırı tespit sistemleri için ilk model değildir. Saldırı tespiti için çeşitli yapay bağışıklık modelleri önerilmiştir [38]. Tüm sistemler bölüm 1' de anlatılan insan bağışıklık sisteminin ayrıntılı yapısının küçük birer alt yapısı oluşturmaktadır. İnsan bağışıklık sisteminin yapısı çok karmaşık olduğundan bunun bilgisayar sistemine tam olarak uyarlanması oldukça zordur.

Bu bölümde oluşturulan yapay bağışıklık sistemi modelinin çalışma açısından en önemli birimi olan negatif seçim algoritması ayrıntılı şekilde sunulacaktır. Daha önce anlatılan negatif seçim mekanizmasının açıklanması yapay bağışıklık sisteminin saldırı tespit mekanizmasını anlamak için önemlidir.

### 6.6.1. İnsan bağışıklık Sisteminin Negatif Seçimi

İnsan bağışıklık sisteminin önemli özelliklerinden biri çeşitliliği ve genel olmasını sürdürme yeteneğine sahip olmasıdır. Bu yetenek az sayıda antikor ile çok sayıda antijen tespit etme yeteneğidir. Birkaç fonksiyonla bu işlemler gerçekleştirilir. Detektörlerin yaşam döngüsü boyunca olgunlaşmış antikorlara dönüşmesi ve saklanması buna örnek bir fonksiyondur. İnsan bağışıklık sistemi iki organı ile detektör kümelerini oluşturur. Bu organlar timus ve kemik iliği' dir. Şekil 6.2' de insan bağışıklık sisteminin detektör kütüphanesi oluşturma işlemi gösterilmiştir.

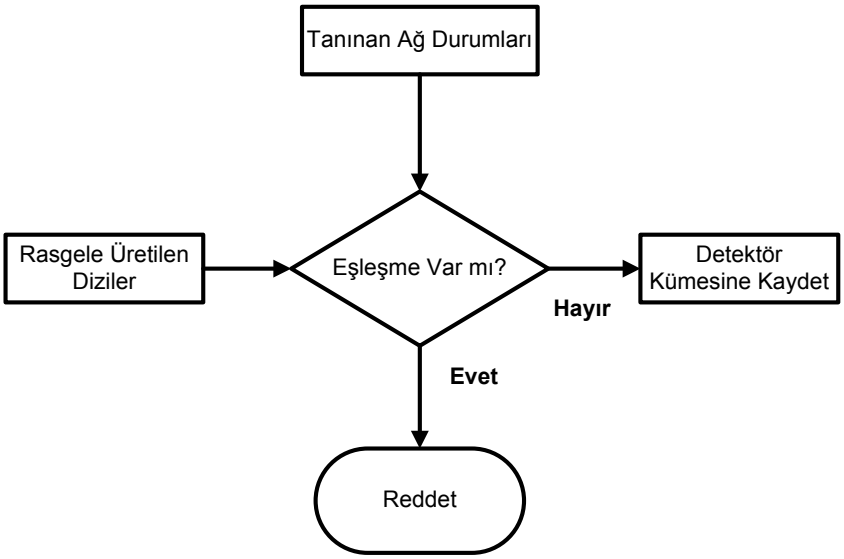



**Şekil 6.2** Detektör Kütüphanesi Oluşturma İşlemi

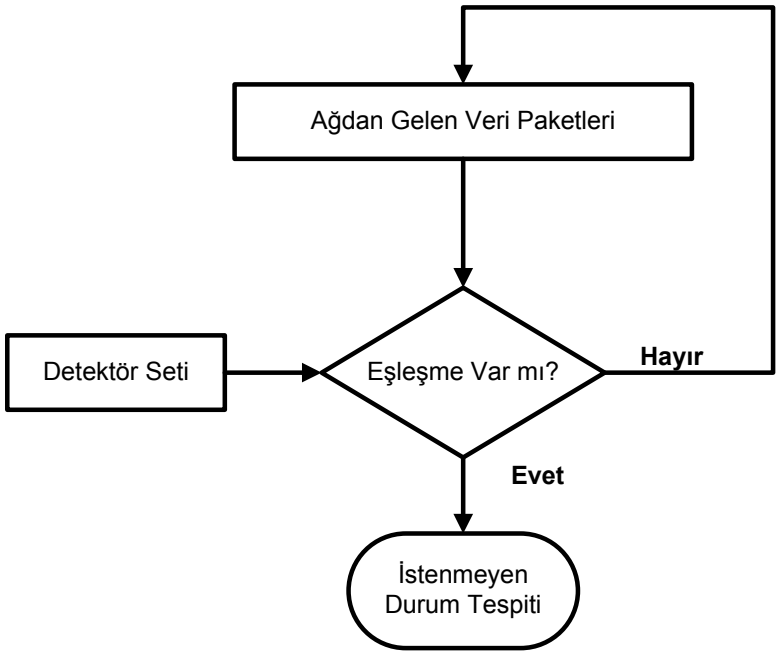
Yeni antikorlar sadece zararlı antijenleri değil aynı zamanda asıl kendi hücrelerini de tespit edebilir. Bu tehlikeleri engellemek için insan bağışıklık sistemi negatif seçimi kullanır. Negatif seçimde olgunlaşmamış antikorlar elenir. Negatif seçim mekanizması insan bağışıklık sisteminin üretilen antikorlar ile kendi hücrelerini saldırı olarak tespit edilmesini engeller.

### 6.6.2. Negatif Seçim Algoritması Çalışma Mekanizması

Anormal detektörlerin tespit edilebilmesi için negatif seçim algoritması kullanılmıştır. Tanınmayan durumların özelliklerini içeren detektörler elde edilir. Kullandığımız ağ saldırı tespit sistemleri için negatif seçim algoritmasını Forrest 1994' de geliştirmiştir [12]. Her bir kullanıcının olağan davranışları tanınan davranışlar olarak isimlendirilir. Şekil 6.3' de Forrest' ın negatif seçim işlemi gösterilmiştir.




**Şekil 6.3** Negatif Seçim Algoritmasının Detektör Seti Oluşturma Aşaması

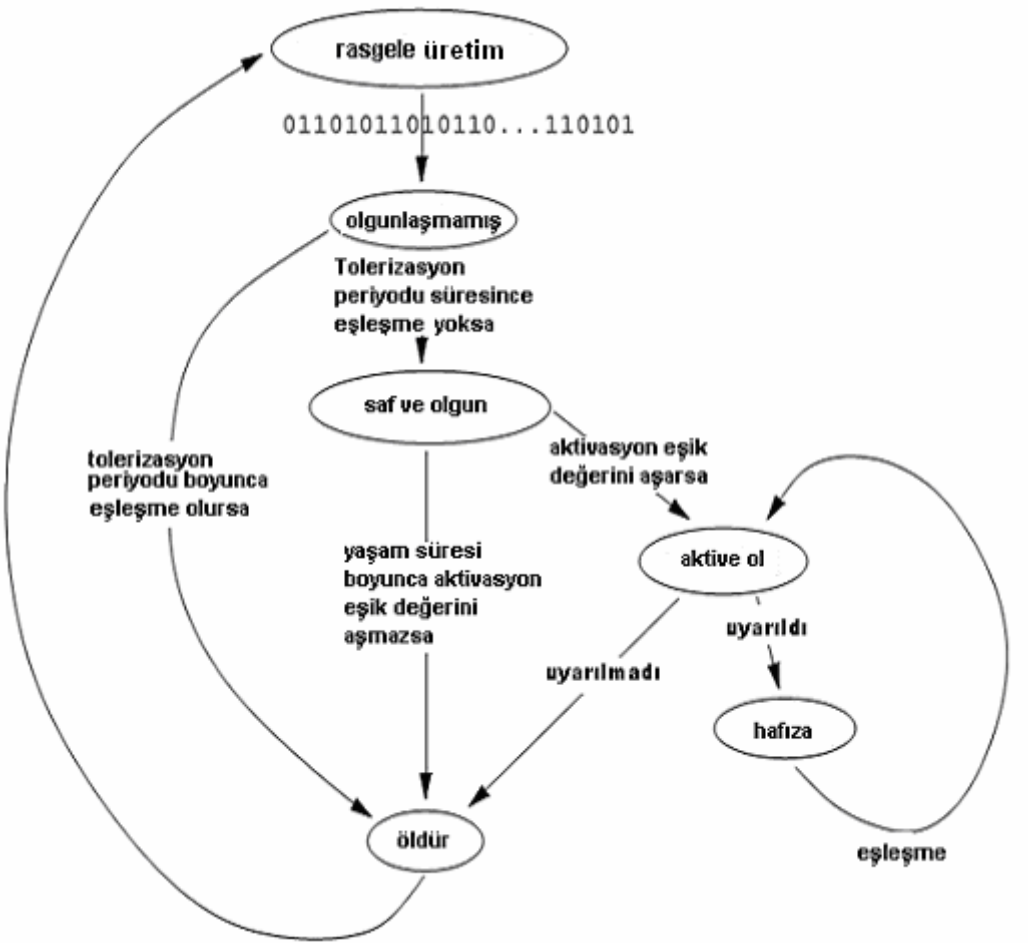



**Şekil 6.4** Detektör Seti ile İstenmeyen Durum Tespit Edilmesi

Çalışmada Forrest'ın önerdiği negatif seçim mekanizması ayrıntılı bir şekilde incelenmiş ve kullanılmıştır [12]. Negatif seçim algoritması iki aşamadan oluşmaktadır. Bunlar detektör kümelerinin oluşturulması ve oluşturulan detektör kümeleri ile istenmeyen durumların tespit edilmesi aşamalarıdır. İlk aşamada rasgele detektör dizileri üretilir. Detektör dizisindeki her bir alanın değeri rasgele üretilir. Oluşturulan detektör dizileri önceden tanımlanan tüm ağ durumlarıyla karşılaştırılır. Eğer detektör dizisi tanımlanan durumlara ait bir tanınan durum dizisi ile eşleşirse o detektör dizisi elimine edilir. Eğer eşleşme olmazsa detektör dizisi uygun detektör olur ve detektör kümesi içerisine kaydedilir. Negatif seçim kabul edilebilir tespit hata oranı ile tanınmayan durum tespiti elde etmek için gerekli seviyeye ulaşacak detektör sayısına kadar bu işlemi tekrar eder. Negatif seçim algoritmasının tanınmayan tespit oranı üretilen detektör sayısı ile doğru orantılıdır. Burada tanınan durumlar ile elde edilen detektörlerin karşılaştırılması önemli bir aşamadır. Birçok araştırmacının kabul ettiği eşleştirme kuralı "r-ardışık bit" kuralıdır [12, 14, 16]. Bu kural iki dizi arasındaki benzer bitlerin sayısını ölçme işlemini gerçekleştirir. Burada amaç mevcut tanınan durumların dışındaki durumları tespit edebilmek için detektör kümeleri oluşturmaktır. Mevcut durumlarla karşılaştırma işlemi yapılarak, istenmeyen durumları tespit edecek, istenilen sayıda detektör kümesi elde edilir.

### 6.6.3. Detektörlerin Yaşam Döngüsü

Detektörler, sistem içerisinde bir yaşam döngüsü içerinde bulunmaktadır. Detektör rasgele oluşturulduktan sonra olgunlaşma sürecine geçer. Tolerizasyon periyodu süresinde olgunlaşmayan detektörler öldürülür. Olgunlaşan detektörler hafıza hücrelerine dönüştürülerek daha sonra karşılaşılacak durumlara karşı saklanmaktadır. İkinci oluşabilecek süreçte hafıza hücreleri rasgele oluşturulan detektörlerin dışında sisteme aktive olacak ve tespit işlemini gerçekleştirecektir. Detektörlerin yaşam döngüsü Şekil 6.5' de gösterilmektedir [14].




**Şekil 6.5** Detektörlerin Yaşam Döngüsü

### 6.6.4. Parametre Ayarları

Parametre ayarları yapay bağışıklık sistemi için önemli bir aşamadır. Yapay bağışıklık sisteminde kullanacağınız detektör sayıları ve elde edilmesi amaçlanan tespit oranlarına karar verilir. Burada sonuçlar elde edebilmek için r-ardışık bit kuralında kullanılacak eşleştirme

uzunluğunun belirlenmesi zorunludur. Bu sayı yaklaşık detektör sayılarını belirlemede kullanılmaktadır. Bu belirleme işlemi (1) ve (2)' de verilen formüle göre hesaplanır [39, 40].

$$P_m \approx m^{-r}[(1-r)\,(m-1) / m+1] \tag{1}$$

$$P_m \approx \frac{1}{N_s} \tag{2}$$

$\boldsymbol{P_m}$ = Detektör dizisi ile rasgele üretilen tanınan durum dizisi arasındaki eşleşme olasılığı

$\boldsymbol{N_s}$ = Tanımlanan durumların sayısı

***m*** = Detektör genotipinin alfabetik gösterim değeri

***l*** = Detektör genotipinin dizi uzunluğu

***r*** = r-ardışık bir kuralında kullanılacak eşleştirme uzunluğu

*m* değeri kullanılacak alfabetik gösterimdeki eleman değerleridir. Çalışmada bu değer 0–1 olup 2 karakter ile gösterilmektedir. *l* değeri detektörün dizi uzunluğudur. $N_s$ değeri tanınan 33 durum sayısıdır. *l* detektör uzunluğu 98 bittir.

$N_s$, *m* ve *l* bilindiğine göre *r* değeri (1) ve (2) kullanılarak hesaplanabilir. Hesaplanan *r* değeri, $N_r$ detektörlerinin yaklaşık sayısını belirlemek için kullanılır. Üretilen deneme detektörlerinin toplam sayısı ise $N_{r0}$, $P_f$ hatalı yanlış tespit oranı sabitlendiği zaman hesaplanır. $N_r$ ve $N_{r0}$, $P_f$ ve *r* değerleri sabit tutulduğunda (3) ve (4) kullanılarak hesaplanır.

$$Nr = \frac{-\ln Pf}{Pm} \tag{3}$$

$$N_{r0} = \frac{-\ln Pf}{Pm\,x\,(1-Pm)^{Ns}} \tag{4}$$

Kullanılacak tekil detektör sayısı için gerekli detektör kümesinin sayısı ve detektör repertuarı Tablo 6.1' de gösterilmektedir.

**Tablo 6.1** Hatalı Tespit Oranlarına Karşılık Gelen Detektör ve Detektör Repertuarı Sayıları

| $P_f$ | $r$=11 | |
|---|---|---|
| | $N_r$ | $N_{r0}$ |
| 0.2 | 53 | 842 |
| 0.1 | 442 | 1204 |
| 0.05 | 575 | 1567 |
| 0.01 | 884 | 2409 |

$N_{r0}$ değeri $N_r$ detektör sayısına ulaşılması için gerekli olan detektör repertuarı sayısını göstermektedir. Sistem içerisinde kullanılacak detektör sayıları belirlenmesi için hesaplamaların yapılması gerekmektedir.

### 6.6.5. Tanımlanan Durumlar

Oluşturduğumuz sistemde TCP protokol kümesi içerisinden elde edilen veri paketlerinin örnekleri çıkarılmıştır. Örnek veri paketleri ağ içerisindeki kullanıcıların normal davranışlarını kapsamaktadır. Paketler TCPDump programı üzerinden elde edilmiştir. Elde edilen veri paketleri kaynak IP adresi, hedef IP adresi, kaynak port, hedef port, paket boyutu, paketin gelme zamanı, protokol tipi gibi bilgileri içermektedir. Bu bilgiler anlamlı veri profilleri oluşturmak için yeterli değildir. Sonuçta asıl normal ve anormal veri durumları belirlemek gereklidir. Birçok araştırmacı TCP protokollerinin güvenlik açıklarını tanımlamıştır [40, 43, 44]. Bu yüzden bizim çalışmamızda temel olarak araştırmalardan elde edilen durumlar kullanılmıştır. Bu araştırmalarda her bir basit bağlantı aktiviteleri tanımlanmıştır. Bu aktiviteler aşağıdaki bilgileri içermektedir.

- **Bağlantı Tanımı:** Her bir bağlantı için dört farklı alan tanımlanmıştır. Bunlar kaynak adres, hedef adres, kaynak ve hedef port' dur. Bu alanlar ilk bağlantının tanımını yapmak için yeterlidir.
- **Saldırı Olabilecek Port Numaraları:** Birçok ağ saldırısı tehlikeye açık portları kullanır. Bu portlar potansiyel tehlikeye maruz olabilecek kaynak ve hedef port bilgileri için gereklidir.
- **Üç Yollu El Sıkışma:** TCP protokolleri bir bağlantı yapabilmek için 3 yollu el sıkışma yöntemini kullanır. Ağ saldırısı olduğu zaman genellikle bu üç yollu el sıkışma yöntemini ihlal eder.

- **Trafik Yoğunluğu:** Ağ aktivitelerinden bir kullanıcı üzerinde olabilecek bağlantı yoğunluğu ölçülebilir. Örneğin paketlerin sayısı, paketlerin boyutu normal bir bağlantıda belirlidir.

Sonuç olarak yapılan çalışmalarda bir ağ üzerinde oluşabilecek normal durumlar 33 farklı veri seti ile tanımlanmıştır. Bu veri kümeleri yapılan çalışmalarından elde edilmiştir [45, 46]. Burada ilk olarak tüm durumlar iç bağlantılar ve dış bağlantılar olmak üzere iki ayrı gruba ayrılabilir. Dış bağlantılar iç kullanıcılar ile dış kullanıcılar arasındaki bağlantıları, iç bağlantılarda ağ içerisindeki kullanıcılar arasındaki bağlantıları belirler.

**Tablo 6.2** Tanımlanan Ağ Durumlarında Kullanılan Alanlar

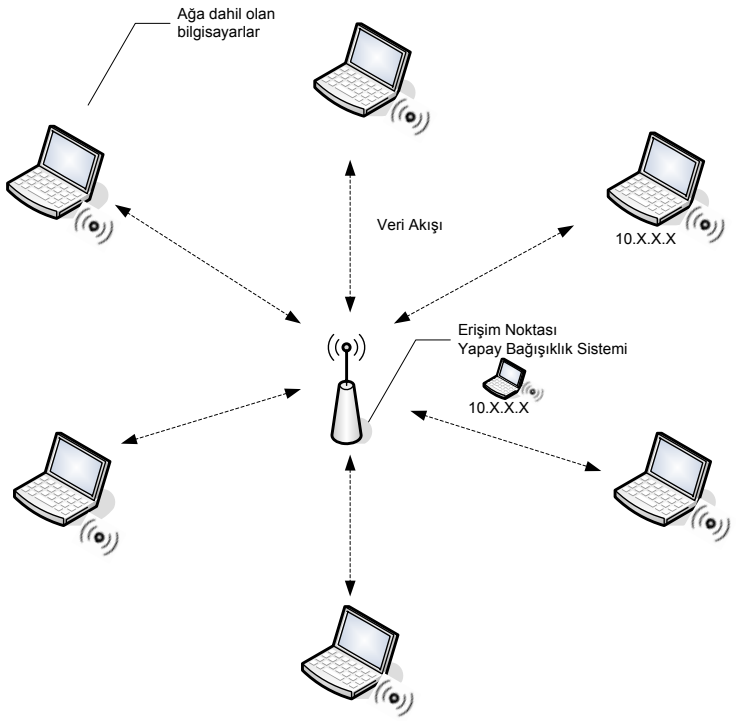
| Alan | Tanımlama |
|---|---|
| *Connection_ID* | Herbir Bağlantının ID Tanımlaması |
| *Src_addr* | Kaynak Adres |
| *Src_Port* | Kaynak Port |
| *Dest_Addr* | Hedef Adres |
| *Dest_Port* | Hedef Port |
| *Server* | Bir kaynak adresi bir server olduğunda doğru |
| *SrcUsr_App* | Bir kaynak portu bir kullanıcı uygulaması kullandığında doğru |
| *SrcPort_Vul* | Saldırıya açık olabilecek Kaynak Portu (5 tane) |
| *SrcPort_firewall* | Güvenlik Duvarları için Kaynak portu (6 tane) |
| *DestUsr_App* | Bir hedef portu bir kullanıcı uygulaması kullandığında doğru |
| *DestPort_Vul* | Saldırı olabilecek Hedef Portu (5 tane) |
| *DestPort_firewall* | Güvenlik Duvarları için Hedef portu (6 tane) |
| *NumberofPacket* | Bir bağlantıda gelebilecek paket sayısı |
| *Duration (Süre)* | Bir bağlantının süresi |
| *PacketRate* | Bir bağlantı süresi içerisinde gelebilecek paket oranı |
| *SentSyn* | Bir bağlantı için Syn Sayısı |
| *SentFın* | Bir bağlantı için Fin sayısı |
| *SentRst* | Bir bağlatnı için Rst sayısı |
| *SentPush* | Bir bağlantı için Push sayısı |
| *SentPushRate* | Bir bağlantı paketleri miktarının push sayısına oranı |
| *Duplicate (Kopya)* | Bir bağlantı için aynı paket sayısı |
| *RateDuplicate* | Bir bağlantıdaki paket sayısını kopya sayısına oranı |
| *Missing* | Bir bağlantıdaki hatalı paket sayısı |
| *RateMissing* | Hatalı paketlerin paket sayısına oranı |
| *OutofOrder* | Bir bağlantıdaki outoforder sayısı |
| *RateOutofOrder* | Bir bağlantıdaki paket sayısının outoforder sayısına oranı |
| *Bytes* | Bir bağlantıda giden paketleri baytları |
| *Bytes rate* | Bir bağlantıda giden paketleri baytlarının bağlantı süresine oranı |
| *Connectionrejected* | Red edilen bağlantı sayısı |
| *Synerror* | Bir bağlantının Synerror sayısı |
| *Termination* | Sonlanma tipi |

| | |
|---|---|
| *WrongSize* | Bir bağlantı içinde bufferı aşan veri gelme boyutu |
| *RateWrongSize* | Bir bağlantı içinde bufferı aşan veri gelme boyutunun bağlantı süresine oranı |

# 7. OLUŞTURULAN KABLOSUZ AĞ SALDIRI TESPİT SİSTEMİ

## 7.1. Kablosuz Ağ Yapısı ve Yazılımın Tanıtılması

Uygulama ortamı olarak kullandığımız kablosuz ağda tüm kullanıcılar aynı anda erişim noktasına bağlıdır. Erişim noktası 108 Gbps hızında ağ sinyali dağıtma yeteneğine sahiptir. Erişim noktasından çıkan sinyal kapalı alanda 100m, açık alanda 400m ye ulaşabilmektedir. Uygulama ortamında 30 kullanıcı ağa dahildir. Kullanıcı bilgisayarları PIV 3.0 Ghz işlemci, 512 MB belleğe sahiptir. Veri paketleri kullanıcı bilgisayarlarından erişim noktasına ulaşmakta ve erişim noktası dağıtım işlemini gerçekleştirmektedir. Kullanıcı bilgisayarlarında ya da ağ cihazlarında herhangi bir güvenlik programı kullanılmamıştır. Erişim noktasının kontrol edildiği bilgisayarın IP adresi 10.1.2.76' dır. Ağ içerisindeki farklı bilgisayarlardan değişik tip tanınan ağ durumlarının dışındaki saldırılar yapılmıştır. Bu saldırılara göre sistemin tespit oranlarına bakılmıştır. Oluşturulan ağ yapısı temsili olarak Şekil 7.1' de gösterilmektedir. Önerilen ağ yapısındaki tüm ağ cihazları Fırat Üniversitesi Bilimsel Araştırma Projeleri birimi tarafından 1167 numaralı Yüksek Lisans Projesi tarafından sağlanan destek ile oluşturulmuştur.




**Şekil 7.1** Temsili Oluşturulan Kablosuz Ağ Yapısı

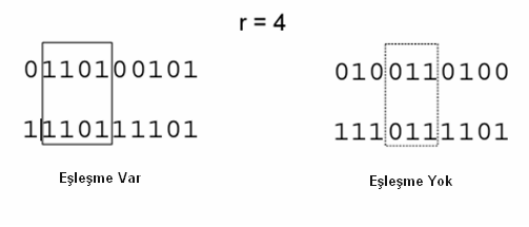
Kontrolün yapıldığı bilgisayar üzerinde Linux işletim sistemi bulunmaktadır. Linux işletim sistemi üzerinde bulunan TCPDump programı ile ağ paket trafiği izlenmiştir. TCPDump

programından ağ üzerindeki tüm paket bilgilerine ulaşılabilmektedir. Bu bilgiler kaynak, hedef IP adresleri, kaynak, hedef port bilgileri, paket boyutu, paketin geliş zamanı, paketin protokol tipi gibi bilgiler bulunmaktadır.

Saldırı tespiti için kullanılan yazılım Forrest ve Hofmeyr' in kablolu ağlarda kullanmış olduğu [1]LISYS programıdır. Bu program ile kablolu ağlarda saldırı tespiti gerçekleştirilmiştir. Fakat Forrest' ın kullanmış olduğu saldırı tespit modeli kullanıcı tabanlı olarak çalışmaktadır. Saldırı tespitini gerçekleştirmek için her bir kullanıcı bilgisayarına uygulama yüklenmiştir. Çalışmada yazılım kablosuz alan ağlarına adapte edilip sonuçlar elde edilmiştir. Uygulamanın çalıştırılabilmesi için Java Sunucunun bilgisayara yüklü olması gerekmektedir. Çünkü kullanılan yazılım Java dili ile yazılmış ve üzerinde esnek ayarlamalar yapabilmek için ihtiyaç vardır. Bu sebeple Java yazılımı uygulamanın kullanıldığı bilgisayara yüklenmiştir. Daha sonra program üzerinde çeşitli parametreler ve kurallar değiştirilerek çalıştırılmıştır.

## 7.2. Karşılaştırma İşlemi ve Detektör Setinin Oluşturulması

Karşılaştırma işlemi için birçok bağışıklık uygulamasında kullanılan "r- ardışık bit kuralı kullanılmıştır. Veri paketleri bitler olarak ifade edilmiştir. Şekil 7.2' de görüleceği gibi iki veri dizisi arasında devam eden bitlerin aynı olması durumunda eşleşme olmaktadır. Eğer devam eden aynı bitlerin sayısı önceden belirlenen bir değere eşit ya da fazla olursa eşleşme meydana gelir. Burada r değeri detektörün tespit etme yeteneğini belirler. Teorikte r=0 olması durumu en genel durum olup tüm basit detektörler eşleşmiş olarak algılanır. Fakat düşük r değerleri tespit etmek için geçen süreyi ve detektör üretim sürelerini arttırmaktadır.




**Şekil 7.2** r- Ardışık Bit Kuralı [14]

Negatif seçim sürecinde daha önceki bölümde anlatılan yapıya uygun şekilde detektörler elde edilir. Detektörler oluşturulurken karşılaştırma işlemi yapılır. Bu karşılaştırma işlemi aşağıda bir örnek ile açıklanmıştır.

***Örnek:*** Önceden tanımlanan bir ağ paketi ile rasgele üretilen bir detektörün eşleştirilip olgunlaşmamış detektörlere dönüştürülmesi aşağıda adım adım gösterilmektedir. Tablo 7.1' de

[1] LISYS programı General Public License [GPL] tarafında patent altındadır. Uygulamanın geliştirilmesi ve kullanılması için açık kaynak kodlu olarak sunulmuş ve herkesin kullanımına izin verilmiştir.

oluşabilecek bir normal durum gösterilmektedir. Bu veri paketi ikilik dizilere dönüştürülerek negatif seçim sürecinde rasgele üretilen detektör dizileri ile eşleştirilmekte ve olgun/hafıza hücrelerine dönüştürülmesi sağlanmaktadır.

**Tablo 7.1** Örnek Veri Yapısı

| Paket Bilgileri | Gösterim Bit sayısı | Örnek Veri |
|---|---|---|
| Kaynak Adres | (32 bit) | 10.1.2.5 |
| Hedef Adres | (32 bit) | 10.1.2.76 |
| Kaynak Port | (16 bit) | 118 |
| Hedef Port | (16 bit) | 348 |
| Protokol (TCP/UDP/ICMP) | (2 bit) | TCP |

Tablo 7.1' de verilen veri yapıları bitsel olarak ifade edilmelidir. Çünkü karşılaştırma için kullandığımız r-ardışık bit kuralı ikilik sayı sistemini kullanmaktadır.

**Tablo 7.2** Verinin Bitsel Olarak Karşılığı

| Örnek Veri | Bitsel Karşılığı |
|---|---|
| 10.1.2.5 | 00001010.00000001.00000010.00000101 |
| 10.1.2.76 | 00001010.00000001.00000010.01001100 |
| 118 | 0000000000111011 |
| 348 | 0000101011110001 |
| TCP | 01 |

Oluşabilecek normal bir durum Tablo 7.2' de verildiği gibi bitler ile ifade edilmiştir. Daha sonra tanımlanan veri dizisi ile rasgele oluşturulan detektörlerin eşleştirme işlemine geçilmiştir. Şekil 7.3' de rasgele üretilen bir detektör gösterilmiştir. Şekil 7.4' de ise tanımlanan ağ durumunun bitler olarak karşılığı gösterilmiştir. Bölüm 6.6.2' de anlatılan negatif seçim işlemi ile bu iki veri dizisi eşleştirme işlemine tabi tutulur. Çalışmada önceden tanımlanması gereken eşleştirme uzunluğu olan r değeri 11 olarak alınmıştır. Çünkü bölüm 6.6.4' de anlatılan hesaplamalara göre bu değer ortaya çıkmaktadır. Kabul edilebilir yanlış tespit oranları belirlendikten sonra uygun eşleştirme için yeterli olan r değeri belirlenir. Bunun sebebi saldırıları tespit edebilecek detektör setinin oluşturulmasında yeterli olmasıdır. Şekil 7.3' de rasgele üretilen bir detektörün ikilik olarak karşılığı gösterilmektedir. Bu ikilik dizi tanınan ağ durumlarıyla karşılaştırma işlemine tabi tutulacaktır. Önceden tanımlanan bir ağ durumu ise Şekil 7.4' de gösterilmektedir.

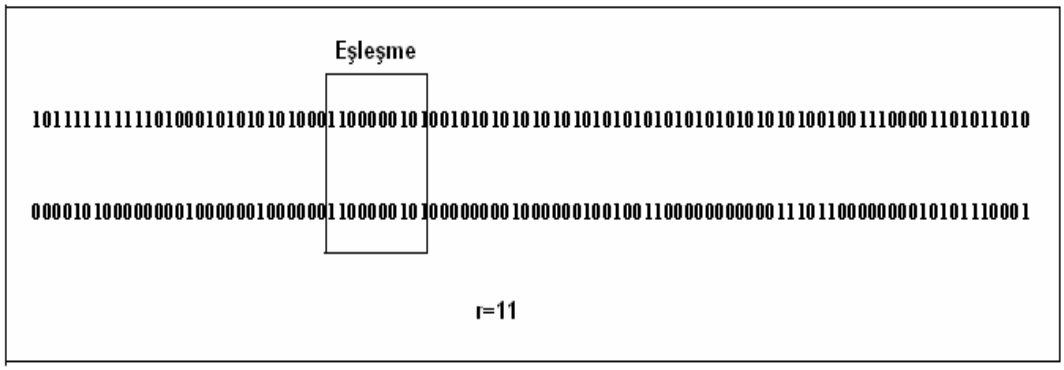
10111111111101000101010101000110000010100101010101010101010101010011110100001101101010110011000101 0

**Şekil 7.3** Rasgele Üretilen Detektör

00001010000000001000000100000010100001010000000010000000100100110000000000001110110000010101110001 01

**Şekil 7.4** Ağ üzerinden Elde Edilen Tanınan Durum Dizisi

Elde edilen veri dizisi ile rasgele üretilen detektörün eşleştirilmesi Şekil 7.5' de gösterilmektedir.




**Şekil 7.5** Örnek Eşleştirme İşlemi

Örnekte görüleceği gibi önceden tanımlanan ağ durumu ile rasgele üretilen detektör dizisi sembolik olarak karşılaştırılmıştır. $r$ =11 değeri için bir eşleşme meydana geldiği görülecektir. Bu durumda rasgele üretilen detektör, detektör kümesine kaydedilir. Eğer eşleşme olmazsa, üretilen o detektör kaydedilmeden sistemden atılır. Bu aşama ile uygun detektör kümesi oluşturulur. Bu işlem elde edilmesi istenilen hatalı tespit oranını sağlayacak detektör kümesi ulaşıncaya kadar devam eder. Hatalı tespit oranı detektörlerin tanınan durumları tanınmayan olarak tespit etmesidir. Oluşabilecek böyle bir durum istenmemektedir. Fakat hiçbir saldırı tespit sistemi yüzde yüz bir tespit gerçekleştiremez, tüm sistemlerde kabul edilebilir hatalı tespit oranlarına göre uygulamalar geliştirilir [39, 40, 45]. İstenilen sayıda detektör sayısına ait repertuar elde edildikten sonra ikinci aşamaya geçilir.

İkinci aşamada eşleşen ve detektör kümesine kaydedilen detektör, ağ üzerinden gelen paketlerle kontrol edilir. Kontrol işlemi için ise r-ardışık bit kuralı kullanılır. Bu aşamada ağdan gelen paketlerle detektör eşleştiği takdirde bu paket saldırı olarak tanımlanmaktadır.

İlk aşamada oluşturulan detektörler bölüm 6.6.3' de anlatıldığı gibi bir yaşam döngüsü içerisindedir. Bu yaşam döngüsü içerisinde olgunlaşmış ve olgunlaşmamış detektör kavramları ortaya çıkmaktadır. Olgunlaşmamış detektörlerin, olgunlaşmış detektörlere dönüşmesi için bir tolerizasyon periyodu geçmesi gerekmektedir. Negatif seçim sürecinde eğer tolerizasyon

periyodu süresince bir eşleşme oluşmazsa bu hücreler artık olgun hücreler haline dönüşür. Eşleşme olduğu takdirde bu hücreler öldürülür. Eğer olgunlaşmamış detektör olarak isimlendirilen bu detektörler önceden tanımlanan bir süre için negatif seçim tarafından silinmezse olgunlaşmamış bu detektörler olgun detektörlere dönüşür. Olgun detektörler gizli anormal durumları ve yeni gelen antijenleri izler. Her bir detektör önceden tanımlanan ve aktivasyon eşiği olarak isimlendirilen bir yeterli sayıda anormal ile eşleşirse uyarı sinyali alır. Bu durumda bu olgun detektörler hafıza hücrelerine dönüşür. Eğer bu sinyal hatalı bir sinyal ise bu detektör öldürülür. Ayrıca olgun detektörler önceden tanımlanan bir süre boyunca anormal tespiti yapamazsa bu detektör elimine edilir. Hafıza hücrelerine dönüşen detektörler, detektör kümesine eklenir. Daha sonra oluşabilecek aynı tip saldırılara karşı hızlı cevap verilmesini sağlarlar. Uygulamada rasgele bir detektör oluşturmak için gerekli kod parçası Şekil 7.6' da verilmektedir.

```
Rasgele detektor{
    my $self = shift;
    my $detector = new String($self->{length});
    my $i;
    for ($i = 0; $i < $self->{length}; $i++) {
      $detector->[$i] = $self->rand_char();
    }
    return $detector;
}

sub match {
    my $self = shift;
    my $string = shift;
    my $detector = shift;

    my $i;
    for ($i = 0; $i < $self->length; $i++) {
      return 0 if $string->[$i] != $detector->[$i];
    }
    return 1;
}
```

**Şekil 7.6** Rasgele Detektör Oluşturulması İçin Gerekli Kod Parçası

### 7.3. Sistem Parametreleri

Kullanılan yazılımda çeşitli sistem parametreleri değiştirilerek gözlemler yapılmıştır. Uygulamanın çalıştırılabilmesi için bazı parametrelerin belirlenmesi gereklidir. Sistem parametreleri Tablo 7.3 'de gösterilmektedir.

**Tablo 7.3** Kullanılan Sistem Parametreleri

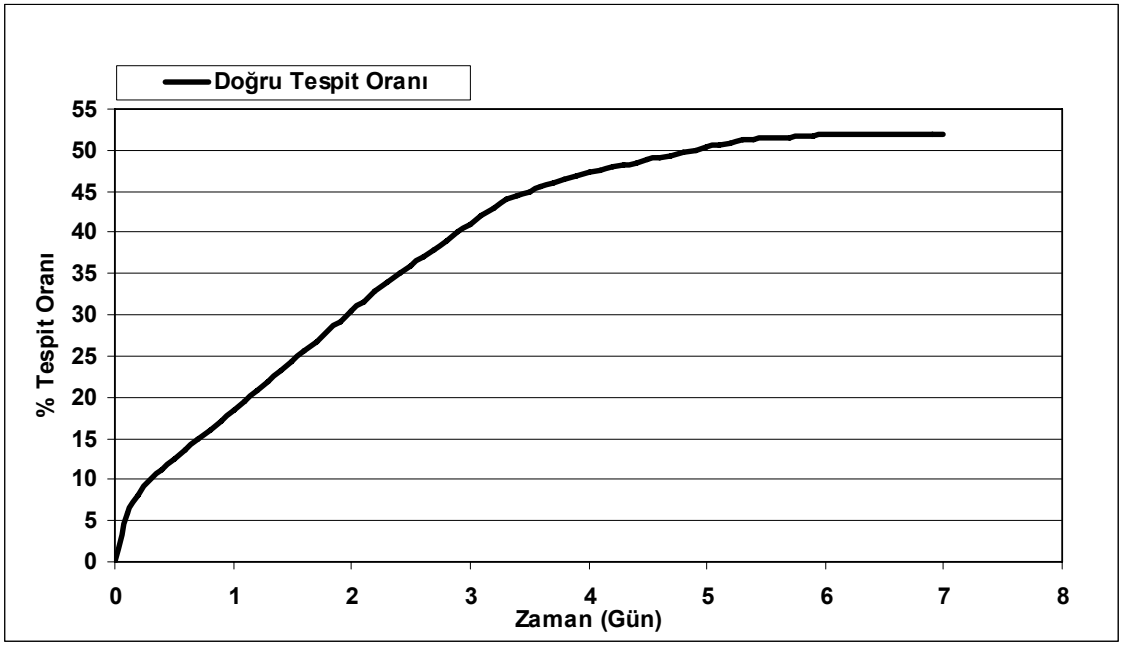
| Sistem Parametreleri | Parametre Değerleri |
|---|---|
| Oluşturulan Olgun Detektör sayıları | 100, 500, 1000 |
| Uygulamanın kullandığı port | 9090 |
| Karşılaştırma Kuralı | r-ardışık bit kuralı |
| Eşleştirme uzunluğu | 11 |
| Aktivasyon eşiği | 5, 10, 20 |
| Maksimum detektör repertuarı | 10000 |
| Uygulama Çalıştırılma Süresi | 7 gün |
| Maksimum kabul edilebilen hatalı tespit oranı | 0,02 – 0,01 – 0,005 |

## 7.4. Uygulamalar

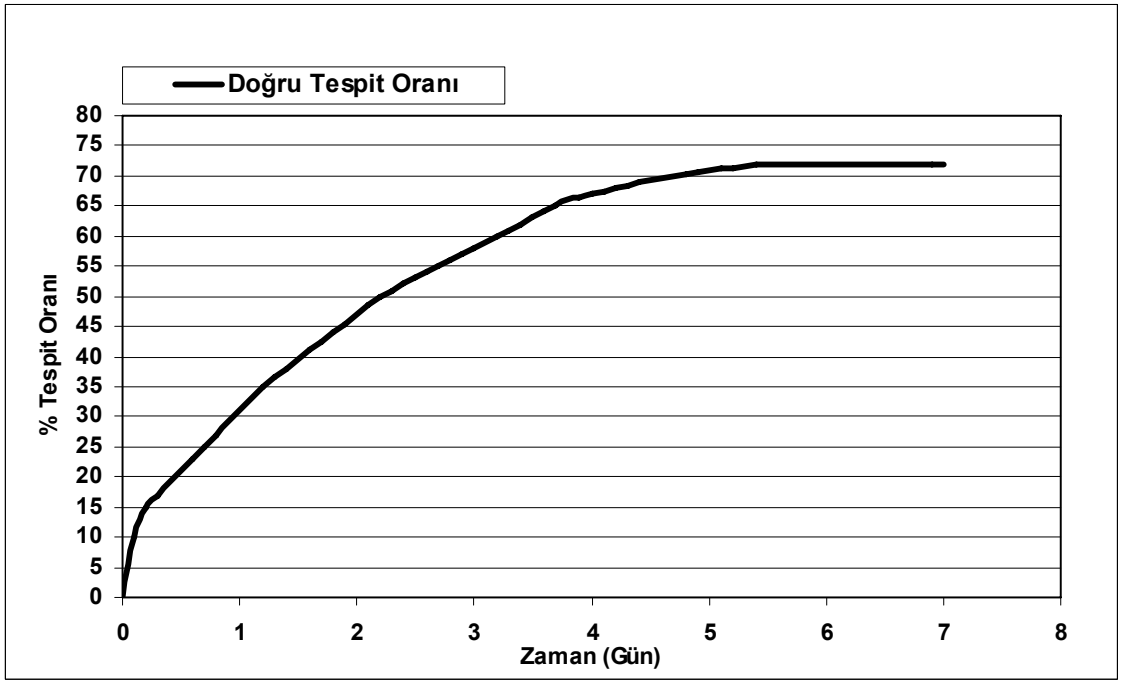
Sistemin çalışmasını test etmek için dört farklı uygulama gerçekleştirilmiştir. İlk uygulamada üç farklı detektör kümesi oluşturulup doğru tespit oranlarına bakılmıştır. Detektör sayıları değiştirilerek tespit oranlarındaki doğruluk farklılıkları gözlenmiştir. İkinci olarak detektör sayısı sabit tutulup aktivasyon eşik değerinin değişimi ile oluşacak sonuçlar gözlenmiştir. Üçüncü olarak saldırı tespiti yapılırken hafıza detektörlerinin kullanılması ile kullanılmaması arasındaki farklara bakılmıştır. Dördüncü uygulama olarak STS' nin verimlilik kapasitesi ölçülmüştür. Saldırı tespit sistemlerinin en önemli olması gereken özelliklerinden biri düşük maliyetlerle çalışmasıdır. Bu nedenle uygulama kullanıcı tabanlı ve erişim noktası tabanlı olarak çalıştırılarak ağın bant genişliği ve ağ cihazlarının performans kayıplarına bakılmıştır. Saldırı tespit sistemlerinin amacı doğru tespit oranları elde etmektir. Eğer yüksek oranlarda doğru tespit oranları elde edilebiliyorsa, STS' nin başarısından söz edilebilmektedir.

### 7.4.1. Uygulama 1

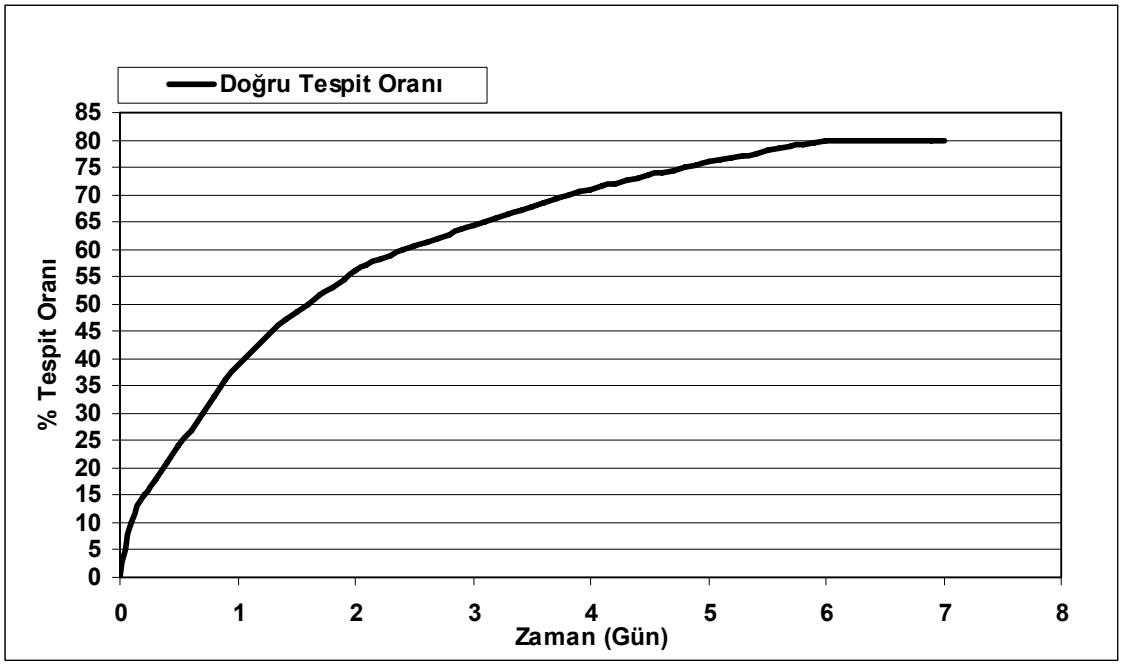
İlk uygulamamızda sistemin tüm parametreleri sabit tutulup detektör sayılarının değiştirilmesi ile elde edilen doğru tespit oranlarına bakılmıştır. D=100, 500, 1000 olarak seçilip uygulama çalıştırılmıştır.




**Şekil 7.7** 100 Detektör ile Tespit İşlemi




**Şekil 7.8** 500 Detektör ile Tespit İşlemi

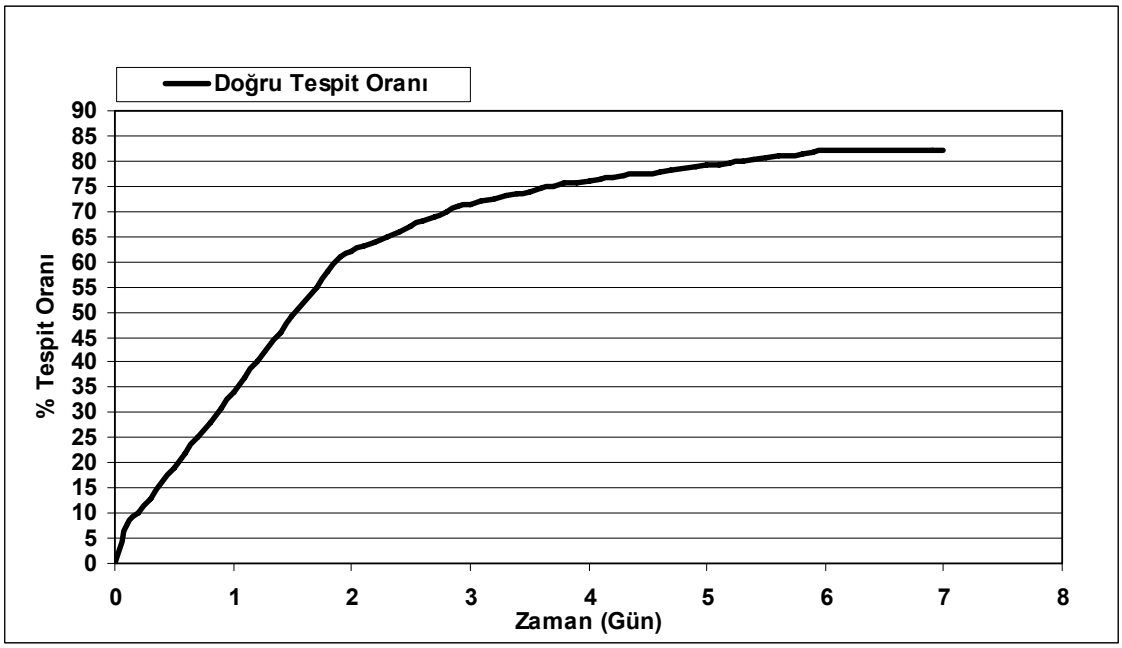



**Şekil 7.9** 1000 Detektör ile Tespit İşlemi

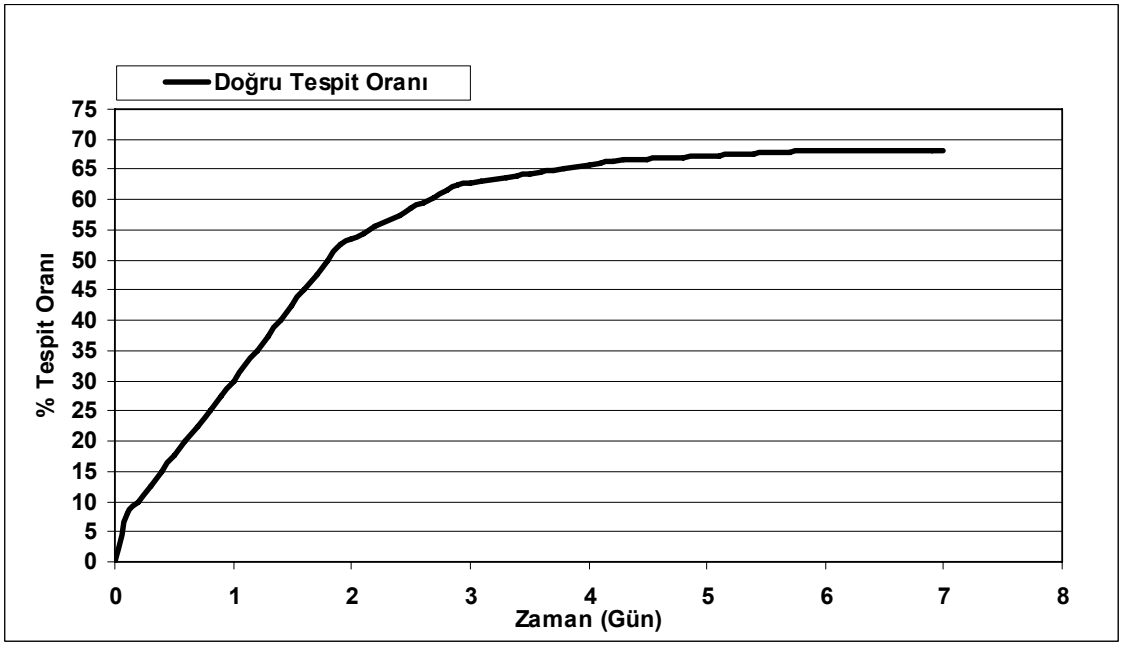
Detektör sayılarının değiştirilmesiyle elde edilen sonuçlar Şekil 7.7, 7.8 ve 7.9' da gösterilmektedir. Detektör sayısının arttırılması doğru tespit oranlarının artmasına sebep olmuştur. Fakat oluşabilecek durum sayısı sınırlı olduğundan belirli bir detektör sayısından sonra tespit oranları aynı seviyeye ulaşmıştır. Fakat burada ortaya çıkan problem, detektör sayılarının artması ile detektörlerin oluşum sürelerinin artmasıdır. Detektör sayılarının artmasının doğru tespit oranlarına etkileri birçok çalışmada da ispatlanmıştır [44-46].

### 7.4.2. Uygulama 2

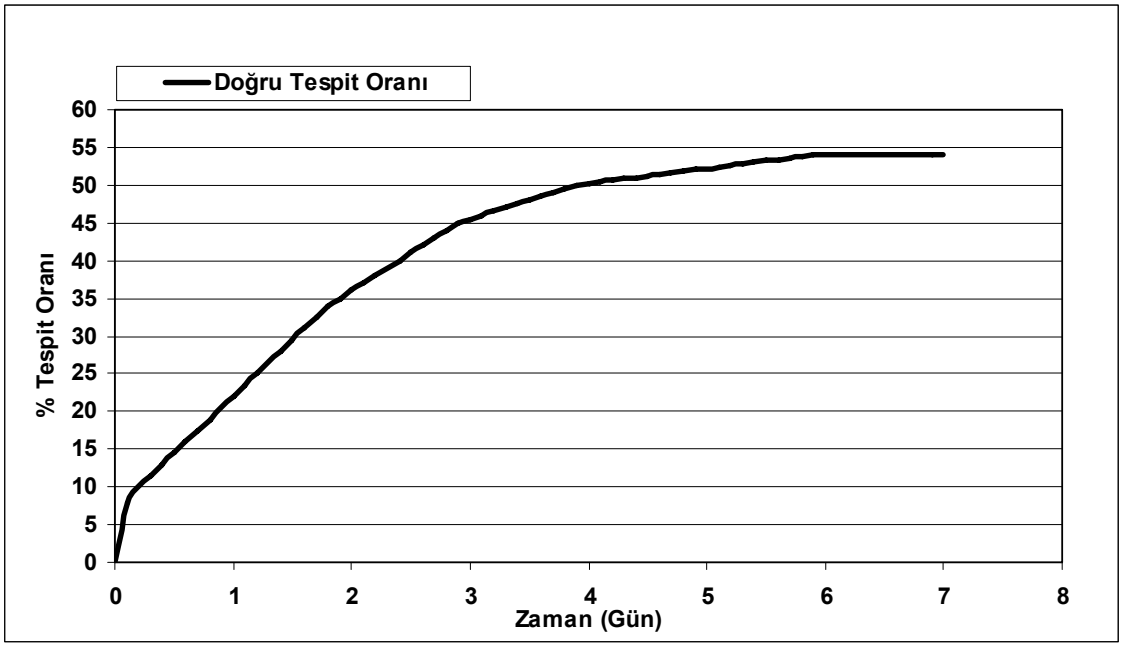
İkinci uygulama olarak detektör sayısı sabit tutulup olgun detektörlerin yaşam döngüsü süresini belirleyen aktivasyon eşik değeri değiştirilmiştir. Bu durumdaki doğru tespit oranların bakılmıştır. Aktivasyon eşik değeri AE=5, 10, 20 seçilmiştir.




**Şekil 7.10** Aktivasyon Eşiği=5 için Tespit İşlemi




**Şekil 7.11** Aktivasyon Eşiği=10 için Tespit İşlemi

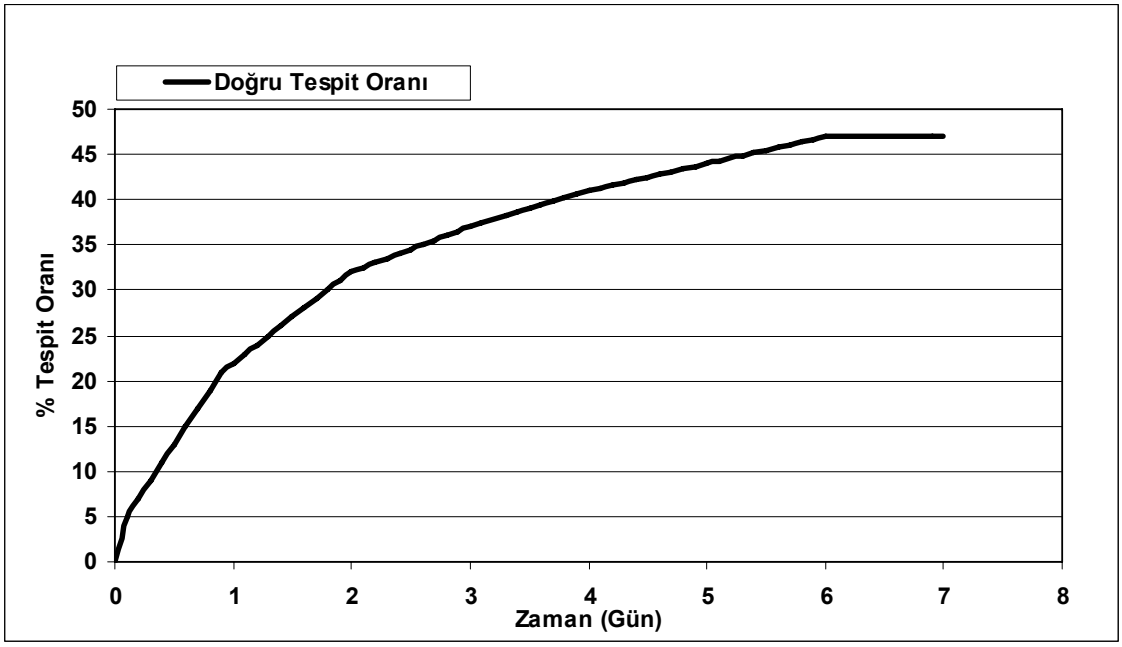



**Şekil 7.12** Aktivasyon Eşiği =20 için Tespit İşlemi

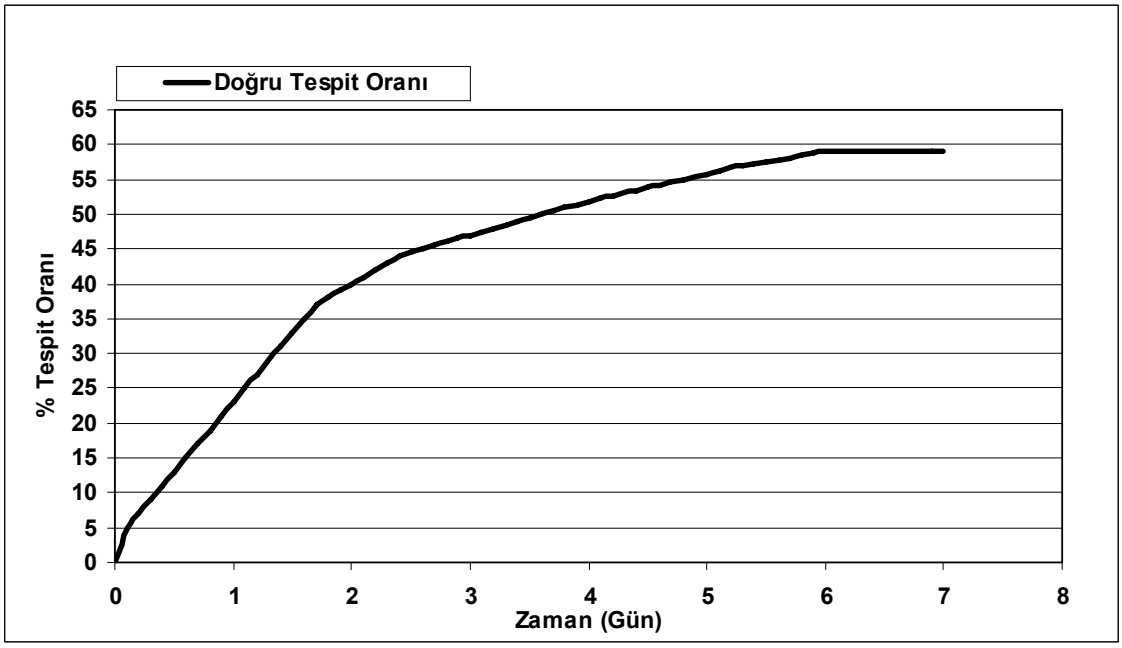
Farklı aktivasyon eşik sürelerine göre elde edilen doğru tespit oranları Şekil 7.10, 7.11 ve 7.12' de gösterilmektedir. Aktivasyon eşik değerinin artması sonucunda doğru tespit oranlarında düşüşler gözlenmiştir. Bunun sebebi aktivasyon eşiğinin büyük olması ile sistemde elimine edilmesi gereken detektörlerin elimine edilmemesi ve bu sebeple doğru tespit oranlarında düşüşe sebep olmasıdır. Yüksek aktivasyon eşik değerlerinde detektörler yanlış tespitler yapabilmektedir. Bunun sonucunda doğru tespit oranlarını düşürmektedir.

### 7.4.3. Uygulama 3

Üçüncü uygulama olarak hafıza hücrelerin kullanılması ile kullanılmaması arasındaki farkları gözlemlemek için uygulama hafıza hücrelerini kullanarak ve kullanmayarak çalıştırılmıştır. İki şekilde çalıştırılan uygulamanın sistem parametreleri aynı tutulmuştur. Bu durumda oluşacak doğru tespit oranlarına bakılmıştır.




**Şekil 7.13** Hafıza Hücresiz Doğru Tespit

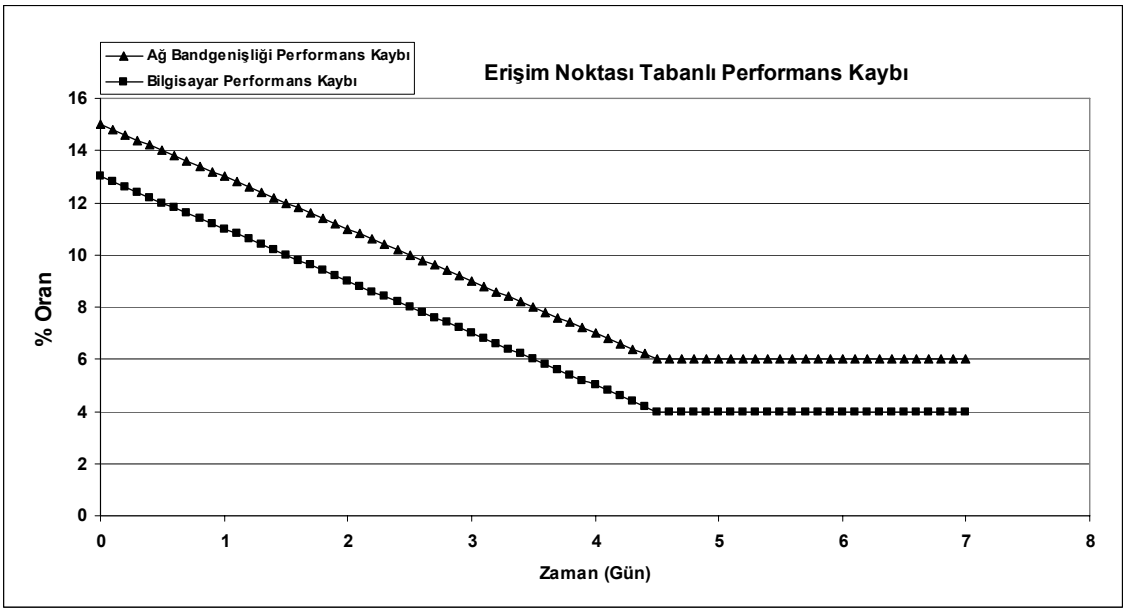



**Şekil 7.14** Hafıza Hücreli Doğru Tespit

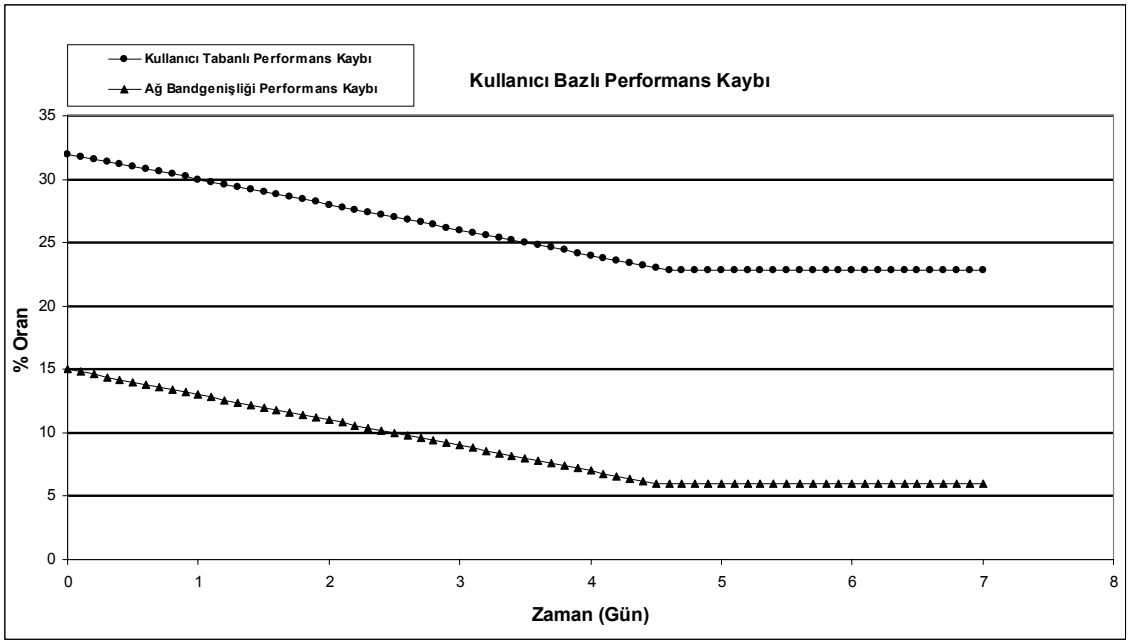
Hafıza hücreleri kullanılarak ve kullanılmayarak elde edile doğru tespit oranları Şekil 7.13 ve Şekil 7.14' de gösterilmektedir. Burada bağışıklık sisteminin en önemli özelliklerinden biri hafıza hücreleridir. Çünkü ikincil bir aynı tip saldırı ile karşılaşıldığında hafıza hücreleri bu duruma karşı hemen tepki gösterebilmektedir. Bu nedenle hafıza hücreleri kullanılarak yapılan tespitte daha doğru tespit oranları elde edilmiştir.

### 7.4.4. Uygulama 4

Dördüncü uygulama olarak YBS değerleri sabit tutularak, uygulama kullanıcı tabanlı ve erişim noktası tabanlı olarak iki şekilde çalıştırılmıştır. Burada kullanıcı tabanlı ve erişim noktası tabanlı saldırı tespiti yapılırken kullanıcı bilgisayarlarının ve ağın bant genişliği kayıpları ölçülmüştür.




**Şekil 7.15** Erişim Noktası Tabanlı Saldırı Tespiti




**Şekil 7.16** Kullanıcı Tabanlı Saldırı Tespiti

Erişim noktası üzerinden yapılan saldırı tespitinden elde edilen tespit oranı Şekil 7.15' de, kullanıcılar üzerinden yapılan saldırı tespitinden elde edilen tespit oranı Şekil 7.16' da gösterilmektedir. Saldırı tespitinin önemli olmasının yanında bilgisayarların ve ağında performanslı bir şekilde çalışması önemli bir kriterdir. YBS' nin uygulama farklılığına göre ağdaki ve bilgisayarlardaki performansı değiştirdiği görülmüştür. Kullanıcı tabanlı YBS' de kullanıcıların bilgisayarlarında önemli oranda performans düşüklüğü gözlenmiştir. Bunun yanında ağ performans düşüş oranları izlenmiştir. Ağ tabanlı YBS uygulamasında ise kullanıcı bilgisayarlarında çok büyük performans kaybı olmadığı görülmüştür. Ağ tabanlı ve kullanıcı tabanlı YBS' nin ağ performans kaybı oranlarına bakıldığında aralarında çok büyük bir farkın olmadığı görülmüştür. Bunun sebebi olarak ağ üzerindeki paket trafiğinde herhangi bir değişikliğin olmamasıdır. Ağ tabanlı ve kullanıcı tabanlı uygulamanın her ikisinde de ağ üzerindeki paketler tüm kullanıcılara ve erişim noktasına ulaşmaktadır. Bu nedenle erişim noktası üzerinden YBS uygulanması daha performanslı olduğu sonucu ortaya çıkmıştır.

### 7.4.5. Uygulama Sonuçları

Uygulamalardan elde edilen sonuçlara göre yapay bağışıklık sisteminin istenmeyen durumları tespit etmedeki başarıları ortaya konulmuştur. Doğru tespit oranları başlangıçta yüksek değildir. Bunun sebebi detektör kümelerinin henüz gelişmemiş olması ve tanınmayan durumları tespit edecek detektör özelliklerine ulaşmamasıdır. Fakat detektör kümesi geliştikten sonra tespit oranları belirli bir seviyeye gelmekte ve aynı seviyeyi korumaktadır. Tespit oranlarının sürekli artış göstermemesinin sebebi oluşturulan detektör kümelerinin detektör

sayılarının sınırlı olmasıdır. Özellikle fazla sayıda detektör kümesi ile tespit oranları doğru orantılı şekilde artmaktadır. Fakat detektörlerin sayısının arttırılması bilgisayar sistemleri için önemli bir sorundur. Detektörlerin üretimleri bilgisayarlarda belirli bir zaman almakta ve fazla sayıda detektörün oluşturulması için gereken süreler oldukça fazladır. Ayrıca hafıza hücrelerini kullanarak yapılan istenmeyen durum tespitleri daha doğru sonuçlar vermektedir. Bu nedenle uygun detektör sayıları seçilerek hafıza hücreleri ile yapılacak tespitler daha doğru sonuçlar vermektedir.

# 8. SONUÇ

Tez çalışmasında yapay bağışıklık sistemi ile kablosuz alan ağlarında saldırı tespiti için bir model sunulmuştur. İlk olarak bu konu ile ilgili daha önce yapılmış olan çalışmalardan iki ana konu üzerine bilgiler toplanmıştır. Bunlar saldırı tespit sistemleri ve bağışıklık sistemidir. Bu çalışmalar ışığında tasarım hedefleri belirlenmiş ve etkin bir erişim noktası tabanlı saldırı tespit sistemi geliştirmek için doğal bağışıklık sisteminin ne gibi özelliklerinden faydalanılacağına karar verilmiştir. İnsan bağışıklık sistemi ile saldırı tespitinde kullanılan öğeler eşleştirilerek etkili ve performans kayıpları az olan bir model önerilmiştir. Bağışık ağ ve tekil antikor kümeleri saldırı tespit sisteminin dağıtık özelliklerini sağlayabilmektedir. Negatif seçim, STS' nin kendi kendine organizasyonunu sağlamaktadır. Böylece genel analiz edilebilirlik ve uyarlanabilirlik gibi faydalar elde edilebilmektedir. Hafıza hücreleri ise STS' nin düşük iş yükleri ile çalışmasını ve daha hızlı cevaplar vermesini sağlamaktadır.

Yapay bağışıklık sisteminin çeşitli sistem parametreleri değiştirilerek elde edilen sonuçlara göre kablosuz alan ağlarında kullanılabilirliği ortaya konmuştur. Ağ ortamına izinsiz girişleri ve sistemi durdurmaya yönelik yapılan saldırıları tespit etmede yapay bağışıklık sistemleri etkin sonuçlar vermiştir. Ayrıca gerçekleştirilen model ile erişim noktası üzerinde tespit işlemi gerçekleştirilerek düşük maliyet ve tüm ağ kontrolü sağlanmıştır.

Kablosuz alan ağ yapısı klasik ağ yapılarına benzerlik göstermektedir. Ancak sınırlı bant genişliği kullanması, sınırlı işlemci gücü, düşük kapasiteli hafızaya sahip olması nedeniyle klasik ağlara getirilen güvenlik yöntemleri kablosuz alan ağ yapılarına doğrudan uygulanamamakta ve etkili sonuçlar elde edilememektedir. Bu nedenle YBS kullanan bir STS başarılı sonuçlar elde edilebileceği bu çalışma ile gösterilmiştir.

Çalışmada genel hatlarıyla bağışıklık sistemi ve yapay bağışıklık sistemi hakkında ayrıntılı bilgileri ile STS çeşitleri ve sınıflandırılmaları verilmiştir. Kablosuz alan ağlarına YBS' nin uygulanma mimarisi gösterilmiş ve uygulamanın çalışma mekanizması gösterilmiştir. Son olarak sistem parametrelerinin değiştirilmesiyle elde edilen sonuçlar verilmiştir. Sonuç olarak YBS kablosuz alan ağlarında saldırı tespiti için kullanılabileceği, fakat sistem parametreleri belirlenirken uygun değerler seçilmesi halinde daha etkili sonuçların elde edilebileceği görülmüştür.

Bu tez çalışması ile Yapay Bağışıklık Sisteminin nasıl bir çalışma mekanizmasına sahip olduğu kavranmış, konu ile ilgili gerekli yayın taramaları gerçekleştirilmiştir. Böylece YBS' nin hangi alanlara uygulanabildiği ve gelecekte yapılacak olan çalışmalara ne gibi faydalar

sağlayacağı kavranmıştır. Son olarak bir YBS uygulaması gerçekleştirilmiş ve sonuçlara ulaşılmıştır.

Gelecek çalışmaları olarak, negatif seçim algoritması ile diğer YBS algoritmalarının bir arada kullanılması ile daha etkin, hızlı ve doğru sonuçlar elde edilebilir. Oluşabilecek istenmeyen ağ durumlarına karşı insan bağışıklık sisteminde bulunan mikropları yok etme özelliği ile engelleme yapılabilir.

**KAYNAKLAR**


1- Seral, Ş., 2004, Yapay Bağışıklıkta Yeni Algoritmalar, Yüksek Lisans Tezi, Selçuk Üniversitesi Fen Bilimleri Enstitüsü, 126s.

2- Baysal, B., 2001, Temel İmmünoloji Ders Notları, Selçuk Üniversitesi Tıp Fakültesi, Mikrobiyoloji Anabilim Dalı, Konya.

3- Abbas, A. K., Lichtman, A. H., Pober, J. S., 1994, Celluar and Molecular Immunology, Fourth ed. W. B. Sounders Com., United States of America

4- De Castro, L. N., and Von Zuben, F. J., 2001, A Pruning Self-Organizing Algorithm to Select Centers of Radial Basis Function Neural Networks, Proceeding of International Conference on Artificial Neural Networks and Genetic Algorithms (ICANNGA'01), 114-117.

5- De Castro, L. N., and Von Zuben, F. J., 2001 , AiNet: an Artificial Immune Network for Data Analysis, (Book chapter in) *Data Mining: A Heuristic Approach*, (Eds) Abbass, H. A., Sarker R. A., Newton, C. S., Idea Group Publishing USA, Chapter XII, 231-259.

6- Kılıçturgay, K., 2003, İmmunoloji, Nobel&Güneş Kitapevi

7- Tizard, I. R., 1995, Immunology: Introduction, 4th Ed, Saunders College Publishing.

8- De Castro, L. N. and Von Zuben, F. J., 1999, Artificial Immune Systems: Part I- Basic Theory and Applications, Technical Report – RT DCA 01/99, 1-95.

9- De Castro, L. Forrest, S., 2002, Information Immune Systems, In Proceedings of the First International Conference on Artificial Immune Systems, University of Kent at Canterbury, ICARIS, UK, 132-140.

10- Ada, G. L. and Nossal, G. J. V., 1987, The Clonal Selection Theory. Scientific American 257(2):50-57

11- Perelson, A. S. & Oster, G. F., 1979 Theoretical Studies of Clonal Selection: Minimal Antibody Repertuarie Size and Reliability of Self-Nonself Discrimination. J. Theor. Biol. 81:645-670

12- Forrest, S., Hofmeyr, S. A., 2000 Immunology as Information Processing. Design Principles for Immune System & Other Distributed Autonomous Systems, Edited By L.A. Segel and I. R. Cohen, eds. Oxford Univ. Pres.

13- De Castro, L.N. and Timmis, J., 2002, A Novel approach to pattern recognition, Computer Science, University of Kent at Canterbury, 64-76

14- Hofmeyr, S. A., Forrest, S., 2000, Architecture for an Artificial Immune System. Evolutionary computation 8(4): 443-473.

15- Akbal, E., 2005, Kablosuz Ağ Teknolojileri ve Yapay Bağışıklık Sistemi, Yüksek Lisans Semineri, Fırat Üniversitesi Fen Bilimleri Enstitüsü

16- Engin, O., Döyen, A., 2004 Artificial Immune Systems and Applications in Industrial Problems, G.U. J. Sci., 17(1): 71-84.

17- De Castro, L. N. and Von Zuben F.J., 2000, The Clonal Selection Algorithm with Engineering Applications, GECCO 2000, Las Vegas, Nevada, USA.

18- De Castro, L. N., Von Zuben, F. J., 2000, Learning and Optimization Using the Clonal Selection Principle. IEEE Transactions on Evolutionary Computation, Special Issue on Artificial Immune Systems.

19- Moscato, P., Fontanari, F.J., 1990, Stochastic versus deterministic update in simulated annealing, Physics Letters A, 146(4):204-208.

20- Costa, A.M., Vargas, P. A., Von Zuben, F. J. and Franca, P.M., 2000, Makespan Minimization On Parallel Processors: An Immune-Based Approach, In the proceedings of the special sessions on artificial immune systems in the 2002 Congress on Evolutionary Computation, 2002 IEEE World Congress on Computational Intelligence, Honolulu, Hawaii.

21- Jensen, M., Hansen, T., 2002, "Robust solutions to job shop problems", http://www.iiuf.unifr.ch/~wangl/immune_reference.html

22- Hart, E., Ross, P., Nelson, J., 1998, Producing Robust Schedules via an Artificial Immune System, ***ICEC***, 464-469.

23- Mori, K., Tsukiyama, M. and Fukuda, T., 1997, Artificial Immunity Based Management System for a Semiconducter Production Line, In IEEE International Conference on Systems, Man, and Cybernetics, 1: 852-856 .

24- Dasgupta, D., Forrest, S., 1999, Artificial Immune systems in Industrial Applications", In the proceedings of the Second International Conference on Intelligent Processing and Manufacturing of materials (IPMM), Honolulu.

25- Lee, D., Jun, H., Sim, B., 1999, Artificial Immune System for Realization of Cooperative Strategies and Group Behavior in collective Autonomous mobile Robots, Proceedings of 4th Int. Symp. On Artificial Life and Robotics:232-235.

26- Dasgupta, D., Forrest, S., 1996, Novelty Detection in Time Series Data Using Ideas From Immunology, Proceedings of the ISCA'96.

27- Ramadin , D., K., Overview of Wireless Broadband Technologies, Intel Corporation http://www.art-telecom.fr/eng/index.htm

28- Autorite de regulation des telecommunications, 2003, WIRELESS LAN, WIFI- A new and decisive change for wireless local area Networks, Paris.

29- Wireless LAN Security Solution http://www.cisco.com/en/US/netsol/ns339/ns395/ns176/ns178/networking_solutions_package.html

30- Gürkaş, G. Z., Durukan Ş., Zaim A. H., Demir A., Aydın M. A., 2005, 802.11b Kablosuz Ağlarda Güvenliğin Ağ Trafiği Üzerindeki Etkilerinin Analizi, II. Mühendislik Bilimleri Genç Araştırmacılar Kongresi, İstanbul.

31- Geier, J., 2002, Wireless LANs, Wireless System Integration, Second edition, Chapter 6, Indiana, ABD, s.1, 5, 7-10, 13

32- Hussain, A., Heidemann, J., Papadopoulos, C., 2004, "Distinguishing between Signal and Multi source Attacks Using Signal Processing", Computer Networks, No. 46.

33- Allen J., Christie A., Fithen W., McHugh J., Pickel J., 1999, State of the Practice of Intrusion Detection Technologies, Tech. Rep. CMU /SEI-99-TR-028.

34- Aydın, M. A., 2005, Bilgisayar Ağlarında Saldırı Tespiti için İstatistiksel Yöntem Kullanılması, Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü 124s.

35- Kemmerer, R.A., Vigna, G., 2002, Intrusion Detection: A Brief History and Overview, IEEE Computer Special Issue on Security and Privacy.

36- Erol, M., 2005, Saldırı Tespit Sistemlerinde İstatistiksel Anormallik Belirleme Kullanımı, Yüksek Lisans Semineri, İstanbul Teknik Üniversitesi

37- Axelsson, S., 2000, "Intrusion Detection Systems: A Survey and Taxonomy", Technical Report Dept. of Computer Eng., Chalmers University.

38- Akbal, E., Ergen, B., 2007, "A Performance Comparison of User and Access Point based Artificial Immune Systems for intrusion detection on a Wireless Local Area Network", International Journal of Computer Science and Network Security (IJCSNS), NO: 7, 119-124

39- Sarafijanovic, S. and Boudec, J., 2005, An Artificial Immune System for Misbehavior Detection in Mobile Ad-Hoc Networks with Virtual Thymus, Clustering, Danger Signal, and Memory Detectors, International Journal of Unconventional Computing, No.1, 221-254.

40- Kim, J. W. , 2002, Integrating Artificial Immune Algorithms for Intrusion Detection, Doktora Tezi, Londra.

41- Balasubramaniyan, J. S., 1998, An Architecture for Intrusion Detection using Autonomous Agents, Department of Computer Sciences, Purdue University, Coast TR 98-05.

42- Somayaji, A., Hofmeyr, S. and Forrest, S., 1997, Principles of a computer immune system, *Proceeding of New Security Paradigms Workshop, Langdale, Cumbria*, 75-82.

43- Buchegger, S. and Le Boudec J. Y., 2003, The Effect of Rumor Spreading in Reputation Systems for Mobile Ad-hoc Networks, In Proceedings of WiOpt `03: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks, Sophia-Antipolis, France.

44- Sarafijanovic, S. and Le Boudec, J.Y., 2005, An Artificial Immune System for Misbehavior Detection in Mobile Ad-Hoc Networks with Virtual Thymus, Clustering, Danger Signal, and Memory Detectors, International Journal of Unconventional Computing, No.1, 221-254.

45- Kim, J. and Bentley, P. J., 2001, Evaluating Negative Selection in an Artificial Immune System for Network Intrusion Detection, Genetic and Evolutionary Computation Conference 2001 (GECCO-2001), San Francisco, 1330 – 1337.

46- Kim, J. and Bentley, P. J., 2001, Towards an Artificial Immune System for Network Intrusion Detection: An Investigation of Clonal Selection with a Negative Selection Operator, the Congress on Evolutionary Computation (CEC-2001), Seoul, Korea, 1244-1252,.

47- Costa, A.M., Vargas, P.A., Von Zuben, F. J. and Franca, P.M., 2002, Makespan Minimization On Parallel Processors: An Immune-Based Approach, In the proceedings of the special sessions on artificial immune systems in the 2002 Congress on Evolutionary Computation, 2002 IEEE World Congress on Computational Intelligence, Honolulu, Hawaii.

## ÖZGEÇMİŞ

1981 yılında Ankara' da doğdu. İlkokul eğitiminin Ankara' da tamamladı. Ortaöğretim ve Lise eğitimini İstanbul' da tamamladı. Lisans eğitimini 2003 yılında Fırat Üniversitesi Elektrik Elektronik Mühendisliği Bölümünde tamamladı. 2004–2005 güz yarıyılında Fırat Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim dalında yüksek lisans eğitimine başladı. Aynı yıl mayıs ayında Fırat Üniversitesi Enformatik Bölümünde okutman kadrosu ile göreve başladı.

Halen Fırat Üniversitesi Enformatik Bölümünde Okutman olarak görev yapmakta ve üniversitenin ihtiyaç duyduğu çeşitli yazılım ve otomasyonları geliştirmektedir.