SALDIRI-BAĞIŞIK AĞLAR

Ağ Güvenliği Dersi

Bahar 2007

Dönem Sonu Projesi

Derleyen: Hasan Esen Kuşluoğlu

İçindekiler Dizini

SALDIRI-BAĞIŞIK AĞLAR....1
1) GİRİŞ....3
2) OMURGALI BAĞIŞIKLIK SİSTEMİ....3
2.1) Doğal Bağışıklık....4
2.2) Edinilmiş Bağışıklık....5
2.3) Bağışıklık Sisteminin Anatomisi....5
2.4) Bağışıklık Sistemi Hücreleri....7
2.4.1) Lenfositler....7
2.4.1.1) B-Lenfositler ve Antikorlar....7
2.4.1.2) T-Lenfositler ve Lenfokinler....7
2.4.1.3) Doğal Öldürücü Hücreler (Katil Hücreler)....8
2.4.2) Yutar-hücreler (Phagocytes), Granülositler ve İlintili Oldukları Diğerleri....8
2.4.3) Tamamlayıcı Sistem....9
2.5) Bağışıklık Sistemi Bedeni Nasıl Korur?....9
2.6) Antikor Molekülü....10
3) YAPAY-BAĞIŞIK DEVRELER....12
3.1) Genel Olarak Yapay-Bağışık Devreler....12
3.2) Saldırı-Bağışık Ağlar....15
3.2.1) Saldırı Bağışık Ağlara İlişkin Kuramlar....16
3.2.1.1) Seçimsel İkizleme....16
3.2.1.2) Haslık Belirlenimi....17
3.2.1.3) Tehlike Teorisi....17
3.2.2) Ağ Güvenliğine Yönelik bir Uygulama Örneği....18
3.2.2.1) Kullanılan Algoritmalar....18
3.2.2.2) İzinsiz Erişim Tespiti....19
4) DÜŞÜNCELER....21
5) KAYNAKLAR:....22

1) GİRİŞ

Son birkaç on yıl içerisinde bilgisayar bilimiyle uğraşanlar, sıklıkla, doğada hali hazırda işler durumda olan yapıları ele almaya ve soyut olarak gerçeklemeye başlamışlardır. Bunun arkasında yatan en önemli sebep, bu yapılara ait mekanizmaların yüksek düzeyde optimize sistemler olmasıdır. Bu yüksek optimizasyon, doğanın milyonlarca yıllık evriminin sonucunda oluşmuş kararlı hallerin bir sonucudur.

Bilgisayar biliminde veya mühendislikte doğadan örnekler kullanılsa da, bunlar her zaman doğanın o sistemi kullandığı biçimde gerçeklenmeyebilir. Bu alanlarda çalışan bilimciler doğadaki biyolojik sistemlerin modellenmesinden çok, geleneksel yöntemlerin baş edemediği problemleri çözmekte kullanmak üzere, bu yapıların işemesini sağlayan çekirdek fikirleri modellemeye çalışırlar.

Biyolojik sistemlerden esinlenerek yapılan modellemeler, aslının kabaca sadeleştirilmiş hali sayılabilecek bir matematiksel modeli olabilir. Buna ilişkin olarak, bir uçak yapmak için kuştan esinlenmeyi veya kurşun geçirmez yelek için örümcek ağlarından esinlenmeyi örnek olarak sayabiliriz.

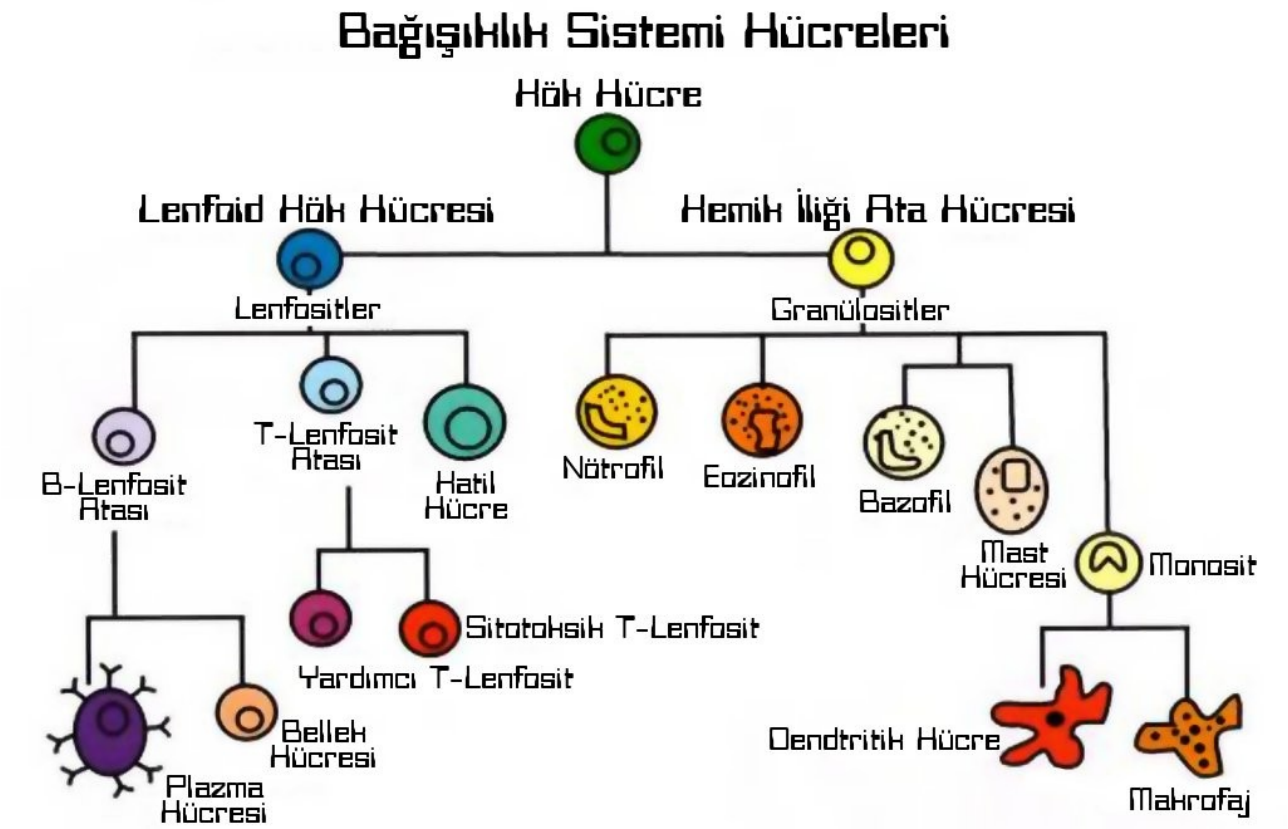
Bu derlemede, omurgalıların biyolojik bağışıklığından esinlenerek gerçeklenmiş Saldırı-Bağışık Bilgi Ağları incelenecektir.

2) OMURGALI BAĞIŞIKLIK SİSTEMİ

Öncelikle, esin kaynağı olan omurgalıların bağışıklık sistemini, temel prensipleriyle ele alalım. Bağışıklık sistemi oldukça karmaşık bir moleküler tanımlama ve tepki sistemidir. Bu sistem sayesinde organizma, kendine has olmayan ögeleri (antijen) birbirinden ayırt etmeyi başarır.

Bağışıklık sisteminin ne kadar başarılı çalıştığını görmek için ölmüş bir canlıya bakmak yeterlidir. Sadece birkaç ay içinde, ölen canlıyı oluşturan neredeyse tüm bileşenler, bağışıklık sisteminin sürekli savaş içerisinde olduğu mikroorganizmalarca sökülür ve sindirilir. Bir insanın ortalama yaşam süresinin 70 yıl olduğunu düşünürsek, bu birkaç aylık çözümlenme süresinin yaşam süresinin yanındaki kısalığı, bağışıklık sisteminin ne kadar güçlü bir savunma mekanizması olduğunu açıkça gösterir. Bu bağlamda, bağışıklık sistemini doğrudan hedef alan tehditlerin de (AIDS gibi) ne kadar ölümcül olabileceği öngörülebilir.

Biyolojik bağışıklıkta rol oynayan hücrelerin genel adı “Beyaz Kan Hücreleri” dir. Bu hücreler şekil de gösterilen şemadaki gibi, kendi aralarında guruplara ayrılırlar.



Bağışıklık sisteminin temel işleyişi B-Lenfosit ve T-Lenfosit Hücrelerine bağlıdır. B-Lenfositler sisteme giren bir patojeni (sisteme yabancı ve zararlı olan istilacılar) tanımlamakla görevine başlar. Sisteme has olmayan ve istilacı olduğu tespit edilen yapılar çevresinde B-Lenfositler, T-Lenfositlerin de yardımıyla hızlı bir mutasyona ve ardından klonlanma sürecine girer. Kabaca ifade ettiğimiz bu olaylar; bağışıklık sisteminin, zararlı olduğu bilinen bir patojeni yok etme ve aynı veya benzer bir patojenin olası yeni saldırılarına karşı kendini hazırlama çabasını tanımlar.

Bağışıklık sistemi, kendi içinde ilintili iki ayrı sistemden oluşur: Doğal bağışıklık ve Edinilmiş (Adaptif) Bağışıklılık.

2.1) Doğal Bağışıklık

Doğal Bağışıklık sistemi her omurgalının doğduğunda sahip olduğu tanımlama ve savunma bilgisidir. Bu bilgiler uzun bir evrimleşmenin sonucudurlar ve kalıtsal olarak yeni doğana aktarılırlar. Bu sayede bağışıklık sistemimiz ilk karşılaşmada bile pek çok patojeni yok edebilecek güçtedir. Doğal bağışıklık sisteminin önemli parçalarından biri, özel bir protein sınıfı olan “*tamamlayıcı sistem”*dir. Tamamlayıcı sisteme ait moleküller, daha sonra ele alınacak olan antikor moleküllerinin (Patojen türü tanımlama ve işaretlemede kullanılırlar) görevlerine yardımcı olurlar.

Doğal bağışıklık sistemi, jerminal merkezlerinde (B-lenfositlerin olgunlaştığı lenf düğümü ve dalakta bulunan özel bölgelerdir.) kodlanan bir gurup örüntü tanımlayıcı almaç (pattern recognition receptor) üzerine kuruludur. Bu almaçlar, mikrobik patojenlerin, üzerlerinde bulundurdukları özel moleküler örüntülerin tanımlanmasını sağlaralar. Bu örüntüler sadece patojenlere özeldir ve asla taşıyıcı beden dahilinde üretilmezler. Bu patojenlerin örüntü tanımlayıcı almaçlarca belirlenmesi bir dizi zincirleme kimyasal tepkimeye sebep olur. Bu tepkimeler patojenin varlığının tespit edildiğine dair sinyalleri taşır. Bağışıklık sisteminin tanımlamaya ait parçalarının kesinlikle bedendeki diğer hücrelerden ve moleküllerden ayrık bir yapıda olması gerekir. Aksi takdirde bedenin kendine ait hücreleriyle, patojenleri birbirinden ayırt edemez. Bu yapının sonucu olarak, doğal bağışıklık, kedine has olan ile olmayanı ayırt edebilir. Başka bir deyişle savunduğu bedene ait olanla olmayanı ayırt edebilir.

Doğuştan bağışıklığın en önemli işlevlerinden biri de yardımcı-uyartı sinyalleri üretmesidir. Bu sinyaller, Edinilmiş (adaptif) Bağışıklık sistemine ait T-lenfositlerin etkinleşmesinde önemli rol oynar.

2.2) Edinilmiş Bağışıklık

Edinilmiş bağışıklık, beden dahilinde, ikizlemeyle (cloning) özel olarak iki tür hücre üzerine dağıtılmış antijen almaçlarını kullanırlar. Söz edilen hücreler, B-lenfosit ve T-lenfosit hücreleridir. Bu hücreler üzerinde bulunan antijen almaçları rastgele süreçlerle üretilirler; ve bunun sonucu olarak, "edinilmiş bağışıklık" tepkisinin tasarımı, seçimsel ikizleme (clonal selection) yoluyla çoğaltılmış, küçük farklılıklarla kendilerine özgü özellikler gösteren almaçlara sahip lenfositlere dayanır [Burnet, 1959-1978]. Bu bağışıklık mekanizması sayesinde beden daha önce hiç karşılaşmamış olduğu patojenlere karşı da kendini savunabilme yetisini kazanır.

2.3) Bağışıklık Sisteminin Anatomisi

Bağışıklık sistemini oluşturan organ ve dokular, beden geneline dağılmışlardır. Bağışıklık sisteminin ana işlevsel parçasını oluşturan beyaz kan hücreleri (leucocytes) dahilindeki lenfositlerin üretildiği, büyütüldüğü ve geliştirildiği yerler lenfoid organlardır.

Lenfoid organlar, birincil ve ikincil lenfoid organlar olmak üzere ikiye ayrılırlar. Birincil lenfoid organlarda, lenfositlerin üretimi işleri yapılırken; ikincil organlarda lenfositler ilk defa antijen uzayıyla yüzleşirler.

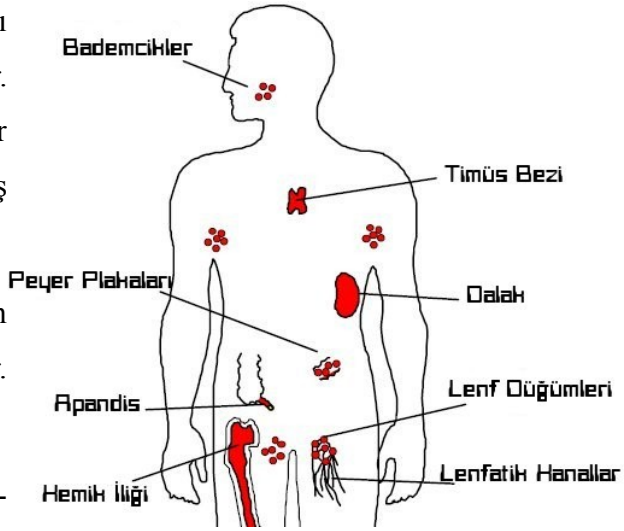
Lenfoid organlar ve ana fonksiyonları aşağıdaki gibidir:

- Bademcikler: Solunum sistemini korumaya yönelik lenf düğümleri ve beraberinde

lenfositleri de içeren yapıdır.

- Lenf Kılcalları: Hücreler arası kimyasal alış-verişi sağlayan şeffaf lenf sıvısının bulunduğu kanallardır.

- Lenf Düğümleri: Lenf sıvısının dolaştığı kılcalların yer yer birleştiği merkezlerdir. Her lenf düğümü B ve T lenfositleri hazır tutar; Bir patojene karşı "edinilmiş bağışıklık" tepkisi bu bölgelerde verilir.



- Kemik İliği: En uzun kemiklerin içlerinde bulunan yumuşak dokudur. Lenfositler ilk olarak burada oluşturulurlar.

- Timüs: Az miktarda lenfosit, olgunlaşmak üzere, kemik iliğinden timüse göç ederler. Timüste çoğalır, olgunlaşır ve T-lenfositlere dönüşürler. T-lenfositler bağışıklık tepkisinin yok edici bileşenleridirler.

- Dalak: Beyaz kan hücrelerinin, kan dolaşımındaki zararlı organizmaları yok ettiği bölgedir.

- Apandis ve Peyer Plakları: Apandis, kalın bağırsağın sonunda bulunun küçük bir ektir. Peyer plakları ise ince bağırsakları çevreleyen lenf dokusu plaklarıdır. Bunlar, sindirim sistemini korumak üzere özelleşmiş bağışıklık hücreleri içeren lenf düğümleridir.

Bağışıklık sistemi kendi içinde "çok katmanlı" bir yapıdadır. Dış dünyadan gelen zararlılar bu katmanlar dahilinde elenirler. Bu katmanları üç gurupta ifade edebiliriz:

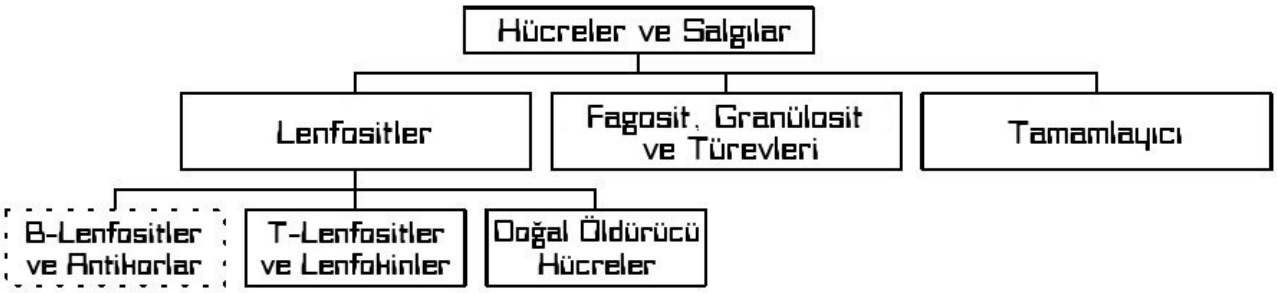
- Fiziksel Engeller: Öncelikle derimiz, iyi veya kötü niyetli istilacılardan bedeni kalkanlar. Solunum sistemi, dışarıdan gelen zararlı maddeleri veya patojenleri, salgıladığı mukus ile tutar. Ayrıca burun kılları da makroskopik zararlıların içeri sızmasını engeller ve hapşırmayı tetikler.

- Fizyolojik Engeller: Tükürük, ter, gözyaşı gibi sıvılar kendi içlerinde yıkıcı enzimler bulundururlar. Ayrıca mide asidi içeri alınan yiyecek ve sudaki zararlıların büyük çoğunluğunu öldürür. Vücut sıcaklığı da bazı bakterilerin yaşamasına engel oluşturacak bir ortam sağlar.

- Doğuştan ve Edinilmiş Bağışıklık: 2.1 ve 2.2 de kısaca bahsedilmiştir.

2.4) Bağışıklık Sistemi Hücreleri

Bağışıklık sistemi, kemik iliğinde üretilen ve çoğunlukla orada olgunlaşan, çok çeşitli hücrelerin bileşiminden oluşur. Kemik iliğinden yola çıkıp, kan dolaşımına, lenflere ve dokulara dağılırlar. Bir kısmı gelen savunma amaçlıyken, diğer bir kısmı çok özel bir patojenle savaşmak üzere özelleşmiştir. Etkin bir savunma için bu hücrelerin sürekli birlikte çalışmaları elzemdir. Aşağıdaki şekilde, bağışıklık sistemini oluşturan hücreler ve salgılar yapısal olarak guruplanmışlardır.



2.4.1) Lenfositler

Lenfositler, bağışıklık sisteminde önemli görevler üstlenen küçük lökositlerdir (Beyaz kan hücreleri). İki ana tür lenfosit vardır: B-Lenfosit (veya B-Hücresi) ve T-Lenfositler. B-Lenfositler, etkinleştikleri zaman, antikor salgılama yeteneği kazanıp plazmositlere (plazma hücresi) dönüşürler.

Lenfositlerin çoğu, uyku durumunda küçük hücreler şeklinde bulunurlar. Ancak kendilerine özgü antijenler ile uyarıldıklarında etkinleşir; ve gerekiyorsa çoğalırlar. B ve T lenfositler, yüzeylerinde, yüksek derecede özelleşmiş antijen tanımlayıcılar bulundururlar. B-Lenfositler üzerindeki almaçlar, uygun tamamlayıcı antijenler ile tamamlandıklarında salgılanacak olan, antikor moleküllerinin hücre zarına bağlanmış bir cinsidir.

2.4.1.1) B-Lenfositler ve Antikorlar

Bakteri, tümör veya virüs gibi bedene has olmayan proteinlerin varlığına cevap olarak, B-Lenfositlerin başlıca görevleri arasında antikor üretimi ve salgılanması olayları ilk sırayı alır. Her B-Lenfosit özel bir antikor üretimi için programlanmıştır. Antikorlar, başka bir özel proteine bağlanmak üzere özelleştirilmiş protein molekülleridir. Antikorların üretimi ve bir yabancı proteine bağlanması; genelde, bağlanılan maddenin, diğer bağışıklık sistemi hücrelerince sindirilmesi/yok edilmesi/öldürülmesi/bağlanılması sinyalini göndermenin yollarından biridir.

2.4.1.2) T-Lenfositler ve Lenfokinler

T-Lenfositlerin “T” si “timüs” bezinden gelir; çünkü timüs bezi, T-Lenfositlerin olgunlaştığı yerdir. T-Lenfositlerin başlıca görevleri, bedene ait hücrelerin gözetilmesi ve enfekte olan hücrelerin yok edilmesi gibi işleri yürütmektir. T-Lenfositleri üç ana alt-gurupta toplayabiliriz:

Bunlar *Yardımcı T-Lenfositler* (Th), *Sitotoksik T-Lenfositler* ve *Baskılayıcı T*-Lenfositler (Supressor T-Lymphocytes) dir.

Yardımcı T-Lenfositler, B-Lenfositlerin, makrofajların ve sitotoksik lenfositlerin etkinleşmesinde önemli rol oynarlar. CD4 veya T4 hücreleri olarak da bilirnirler.

Sitotoksik T-Lenfositler, çeşitli mikrobik istilacıları, virüsleri, kanserli hücreleri yok edebilme yeteneğine sahiptirler. Bir kez etkinleşip, *ligand*larına bağlandıklarında, hücre zarını delip, zararlı hücrenin içine öldürücü kimyasallarını boşaltırlar.

Baskılayıcı T-Lenfositler bağışıklık cevabının yönetilmesinde hayati rol oynarlar. CD8 hücreleri olarak da bilinirler ve diğer lenfositlerin etkinliğini baskılarlar. Bu hücreler olmadan bağışıklık sistemi kontrolünü tamamen yitirebilirdi ve allerjik reaksiyonlara veya otoimmün hastalıklara sebep olabilirdi.

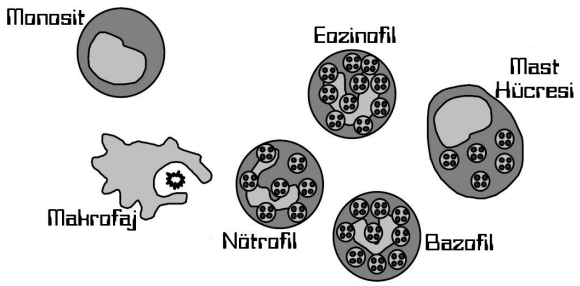
T hücreleri, birincil olarak, *sitokin* veya daha özel adıyla *lenfokin* denen bazı kimyasallar salgılayarak çalışırlar. Bu kimyasallar son derce güçlü mesajcı moleküllerdir. Lenfokinler, hücresel büyüme, etkinleşme ve çoğalma emrini taşırlar; ayrıca düzenleyici (regülatif) özellikleri de vardır. Bunların yanında, lenfokinlerin hedef hücreleri öldürebilme özellikleri veya *Yutar-hücre*leri etkinleşmeleri için uyarabilme işlevleri de vardır.

2.4.1.3) Doğal Öldürücü Hücreler (Katil Hücreler)

Katil hücreler, yok edici hücrelerin diğer bir türünü oluştururlar. Sitotoksik T-Lenfositler gibi, bu hücreler de içlerinde güçlü kimyasallar içeren tanecikler bulundururlar. T-Lenfositlerden farklı olarak, bir hücreyi yok etmek için özel bir antijeni tanımalarına gerek yoktur. Bu hücreler genellikle tümörlere ve virüs bulaşmış hücrelere saldırırlar; ayrıca, büyük miktarlarda lenfokin salgılarlar ve bağışıklık sisteminin düzenlenmesinde etkin rol oynarlar.

2.4.2) Yutar-hücreler (Phagocytes), Granülositler ve İlintili Oldukları Diğerleri

Yutar-hücreler (Fagosit) antijenik parçacıkları ve mikroorganizmaları içine alma ve sindirme yetisine sahip beyaz kan hücreleridir. Bazı Yutar-hücrelerin önemli bir görevi vardır; sindirdikleri patojene ait antijen parçalarını lenfositlere tanıtırlar. Bunlara *antijen-tanıtıcı* hücreler denir.



Önemli yutar-hücreler monositler ve makrofajlardır. Monositler kanla beraber dokulara hareket ederler ve dokularda makrofajlara (büyük yutucular) dönüşürler. Makrofajlar değişik işlevleri olan

çok amaçlı hücrelerdir. Bağışıklık tepkisinin başlamasında önemli yerleri vardır. Karşılaştıkları patojenlere ait antijenleri içlerine alıp sindirdikten sonra T-Lenfositlere tanıtırlar.

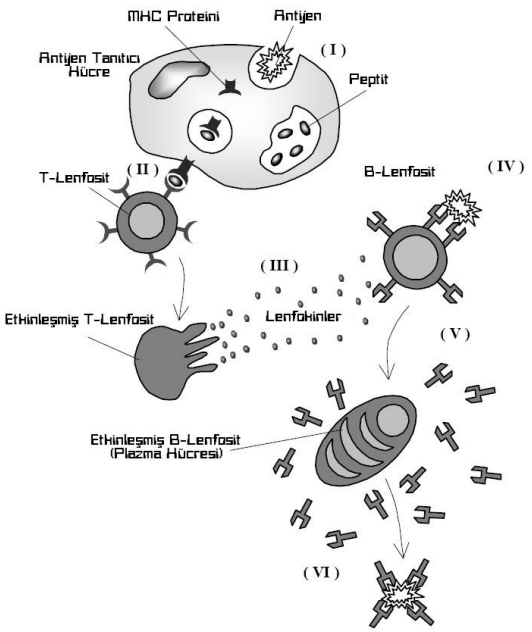
*Nötrofil*ler ve *eozinofil*ler de makrofajlara benzer özellikler gösteren yutar-hücrelerdir. *Bazofil*ler *mastosit*ler farklı üretim süreçlerinden geçmelerine rağmen benzer işlere yarayan, içlerinde kuvvetli kimyasallar bulunduran tanecikler içeren hücrelerdir. İnflamatuar reaksiyonların başlamasında etkindirler. Mastositler solunum yollarının dış dünyayla temas ettiği dokuların altında yoğunlukla bulunurlar.

2.4.3) Tamamlayıcı Sistem

Tamamlayıcı sistem (Complement System), kanla birlikte dolaşan ve antikorların işlevini tamamlayıcı özellikler gösteren bir plazma proteinleri gurubudur. Tamamlayıcı sistem istilacı bir organizma tespit ettiğinde, her bileşeni bir zincirleme tepkimeyi körükleyici davranış gösterirler. Bunun sonucunda istilacı organizmanın hücre duvarına bağlanan protein kompleksleri lezyonlar oluşmasına sebep olur. Bu işler, yutar-hücrelerin sindirme işlerini kolaylaştırır. Beden genelinde uyur halde gezinen yaklaşık 25 farklı protein molekülünden oluşur.

2.5) Bağışıklık Sistemi Bedeni Nasıl Korur?

Genel olarak toparlarsak, daha önce de belirtildiği gibi, bedenimiz, kendi içinde etkileşimli çeşitli hücre ve molekül ordularıyla korunur. Bütün bağışıklık tepkilerinin hedefi (ve sebebi) olan yabancı antijenler, bir bakterinin veya başka bir istilacının üzerinde bulunurlar.



Makrofajlar gibi, özelleşmiş antijen-tanıtıcı hücreler, vücut dahilinde sürekli dolaşırlar ve karşılaştıkları antijenleri içlerine alıp sindirerek antijenik peptitlere ayırırlar (I). Bu peptit parçaları MHC molekülüne (Major Histocompatibility Complex) eklenirler ve ayrıca hücre yüzeyinde de gösterilirler. T-Lenfositler üzerlerinde değişik peptit-MHC kombinasyonlarına duyarlı almaçlar bulundururlar (II). T-Lenfositler bu tanımlama işlemi sonucunda bölünür ve bağışıklık sisteminin diğer elemanlarını harekete geçirecek olan lenfokin veya kimyasal sinyaller salgılarlar (III). B-Lenfositler üzerlerinde tek tür özelleşmiş almaç moleküller bulundururlar ve bu sinyallerle etkinleşirler. T-Lenfositlerin aksine, B-Lenfositler bir çözelti içindeki antijen parçalarını MHC molekülü olamadan tanımlayabilecek yetenektedirler(IV).

B-Lenfositler etkinleştikleri zaman bölünür ve almaç moleküllerinin çözünür şekli olan antikorları salgılayan plazma hücrelerine dönüşürler(V). Antikorlar, buldukları antijenlere bağlanarak onları etkisizleştirirler (VI) veya tamamlayıcı sistemin enzimlerinin ya da devriye gezen çöpçü hücrelerin, üzerlerine hücum etmesine sebep olarak yıkımlarına sebep olurlar.

Bazı B-Lenfositler *bellek hücrelerine* dönüşür ve kan dolaşımında uzun süre kalırlar. Bu sayede aynı veya benzer bir patojenin ikinci bir saldırısına karşı bağışıklık tepkisi daha hızlı ortaya konabilir. B-Lenfositlerde Antikor üretimi için kullanılan genler sürekli mutasyona ve düzenlemeye uğradığından, tekrar eden saldırılar karşısında antikor cevabı eskisine göre daha etkin ve net bir hal almaya başlar. Bu olaya *eğilim olgunlaşması* (affinity maturation) denir.

2.6) Antikor Molekülü

Bağışıklık sistemi içinde, antikor molekülü, çeşitli antijen moleküllerin algılanması ve tanımlanması sürecinde merkezi bir rol oynar. Antijenler son derece çeşitli olduklarından bağışıklık sisteminin tanımama listesinin son derece geniş olması gerekir. Bu kadar çok ve birbirinden farklı -yine de birbiriyle ilintili- proteinleri kodlamak ve saklamak için kullanılan genetik bilgi germ (tohum) türü hücrelerde depolanarak nesiller boyunca aktarılır.

Bir antikorun (veya immünoglobülin) temel birimi, birbirinin ikizi iki hafif zincirden ve yine birbirinin ikizi iki ağır zincirden oluşur. *Değişken Bölge* olarak adlandırılan V-Bölgesi öncelikli olarak antijen tanımlaması işinden sorumludur ve bu kısma ait olan değişken alt-bölgelere ait artık kısımlar gerçekten antijen temasında bulunan kısımlardır. Bu alt-bölgeler "tamamlayıcılık belirleme bölgesi" (complementarity determining regions - CDRs) olarak adlandırılırlar. *Sabit bölgeler* (C) ise tamamlayıcı sabitlemesi (complement fixation) gibi çeşitli dengeleyici işlevler üstlenirler. Bir immunoglobülin poli-peptit zinciri, germ soyundan bir hücrenin genomundaki kromozomların içindeki gen bölütlerinden kodlanır. B-Lenfositlerin içinde tam ve etkinleşmiş bir immünoglobülin geninin oluşturulabilmesi için bu gen bölütlerinin bir araya getirilmesi şarttır. Buna bağlı olarak, çeşitlenmeyi artırıcı mekanizmaların birinden bahsedebiliriz: Rekombinasyon... B-Lenfositler bölünerek çoğalma emrini aldıklarında, bir rekombinasyon sürecinden de geçerler. Bölünme sırasında kendi genomunu ikizleyen B-Lenfosit, aynı anda antijenlerin değişken bögelerine denk gelen gen bölütlerine ait kısımları da kendi arlarında takas edip yeni kombinasyonlar üretir. Başka bir deyişle, B-Lenfositlerin kendilerini çoğaltma işlemi, gen bilgisi açısından birebir bir ikizleme değildir. Bunun yanında, immünoglobülin genleri yüksek miktarda somatik mutasyona (somatic hypermutation) da uğrarlar. Bu tür mutasyonlar sadece bağışıklık sistemine özgü hücrelerde görülür.

Antikor genlerinin çeşitlenmesi için iki farklı mekanizmanın evrimleşmiş olması dikkat çekicidir. Neden aynı işi yapmak için iki farklı mekanizma evrimleşmiştir? İki mekanizmada B-Lenfositlerin gelişimi süresince sıkı denetim altında tutulur. İmmünoglobülin genlerinin rekombinasyon süreci ilk sırada gerçekleştirilen iştir ve B-Lenfositlerin antijenlerle ilk yüzleşmelerinden önce tamamlanır. Bu süreç, özellik olarak son derece geniş bir yelpazede çeşitlenmiş, ve fakat, içlerinden sadece birkaç tanesinin hedef antijeni tanımlayabildiği, yeni B-Lenfosit hücreleri üretir. Bu aşamadan sonra somatik hipermutasyon devreye girer. Hedef antijeni tanımlayabilen B-Lenfositler seçilir ve bu guruptan ikinci nesil hücreler üretilir. İkinci nesil çoğalma sırasında, B-Lenfositlerdeki antikorların, değişken bölgelerine ait genlerin, büyük bölütler halinde yer değiştirmesi yerine; bu bölütlerdeki nükleotid bazlarında ekleme, çıkarma, yer değiştirme gibi işlemler yapılarak çeşitlilik sağlanır. Bu şekilde, bir bakıma, tanımlama yetilerine ince-ayar yapılmış olur.

Buraya kadar bağışıklık sisteminin genel yapısı ve işleyişi hakkında fikir sahibi olmaya çalıştık. Bağışıklık sistemi konusun hala pek çok karanlık noktalar ve ateşli tartışmalar içeren bir konudur. Bu derlemede “özetin özeti” denebilecek şekilde bağışıklık sistemi ve yetenekleri irdelenmeye çalışılmıştır. Bu noktadan sonra, bu sistemin matematiksel modellemesi ve bu tür modellemelerin kullanım alanları konusunda yine özet sayılabilecek nitelikte, genelden özele giderek, ağ güvenliğine yönelik çalışmalara doğru yolumuzu çizmeye çalışacağız...

3) YAPAY-BAĞIŞIK DEVRELER

Son birkaç sene içerisinde, bilgisayar bilimcileri, mühendisler, matematikçiler, filozoflar ve diğer alanlarda çalışan araştırmacılar, Omurgalı bağışıklık sisteminden esinlenilerek ortaya atılan "Yapay-Bağışık Devreler" (Artificial Immune Networks) fikriyle daha çok ilgilenmeye başladılar. Bu ilginin artışı, konunun yeni bir araştırma alanı olmasına sebep oldu.

Omurgalı Bağışıklık Sisteminin pek çok özelliği aşağıdaki sebeplerden dolayı bilgisayar bilimcilerinin ilgisini üzerinde toplamıştır.

- Eşsiz Olma: Her canlının kendi bağışıklık sistemi vardır.
- Haslık Belirlenimi: Bedene ait olmayan zararlı moleküllerin (antijen) ayrımına varabilme.
- Anormallik Tespiti: Bağışıklık sisteminin daha önce hiç karşılaşmamış olduğu bir zararlıya tepki vermesi.
- Dağıtık İşleyiş: Bağışıklık sistemini oluşturan hücreler bedenin her kademesinde etkindirler ve merkezi bir işleyişleri yoktur.
- Gürültü Tolerası: Zararlıların net tanımlamasının bilinmesi zorunlu değildir; sistem esnektir.
- Etkiyle Öğrenme ve Bellek: Bağışıklık sistemi, sonraki olası bir karşılaşmada daha çabuk tepki vermek için zararlıların yapısını öğrenebilir. Benzer zararlılara da tepki verebilir.

3.1) Genel Olarak Yapay-Bağışık Devreler

Bu kısımda, Yapay-Bağışık Devreler kuramını, özel bir modele odaklanmadan, genel olarak ifade etmeye çalışacağız. Bu konuya ilişkin bazı model ve yaklaşımlar, Hoffmann (1975); Richter (1975, 1978); Bonna & Kohler (1983); Coutinho et al. (1984); Jerne (1984); Langman & Cohn (1986); Farmer et al. (1986); Segel & Perelson (1988); Perelson (1988, 1989); Coutinho (1989, 1995); Varela & Stewart (1990a,b); Stewart & Varela (1991); De Boer & Perelson (1991); Calenbur et al. (1995); Detours et al. (1996); Bernardes & dos Santos (1997); Perelson & Weisbuch (1997) adlı bililimcilerin çalışmalarında ele alınmıştır.

Yapay-Bağışık Devreler kuramı ilk önerildiğinde (Jerne, 1974), ne hücreler arası işaretleşmeyi ne antikor ve hücreler arasındaki etkileşimleri açıklamayı, ne de bu etkileşimler sonucunda etkinleşen tepki mekanizmalarını açıklamayı hedefliyordu. Bunun yerine, lenfosit etkinlikleri, doğal antikor üretimi, bağışıklık öncesi kitaplık seçimini, tolerans ve haslık belirlenimini, bellek ve bağışıklık sisteminin evrimleşmesini açıklama yönünde fikirler ortaya koyuyordu (Varela & Coutinho, 1991).

Yapılan önermeler genel olarak, bağışıklık sisteminin, ortamda antijenler olmadığı halde bile birbirlerini tanıyan, kendi kendini ayarlayabilen bir moleküler devre olduğu yönündeydi. Bu bakış açısı o zamanlar kabul gören "seçimsel kuram" (selective theory) ile çelişir bir yaklaşımı temsil ediyordu. Seçimsel kuram, bağışıklık sistemini, başlangıçta atıl durumda olan, sadece bir antijenle karşılaştığında tetiklenen, birbirinin ayrık ikizleri halinde bir hücre seti olarak kabul ediyordu.

Antikor üretimi sırasındaki rastgele süreçleri daha sonra incelemek üzere, şimdilik göz ardı ederek "haslık" belirlenimini açıklamaya çalışan fikirleri ele alarak devam edelim. Sözünü ettiğimiz bu öncü çalışmalarda öncelikle bazı tanımlamalar yapılma yoluna gidilmiştir. Bu tanımlamalar şöyledir:

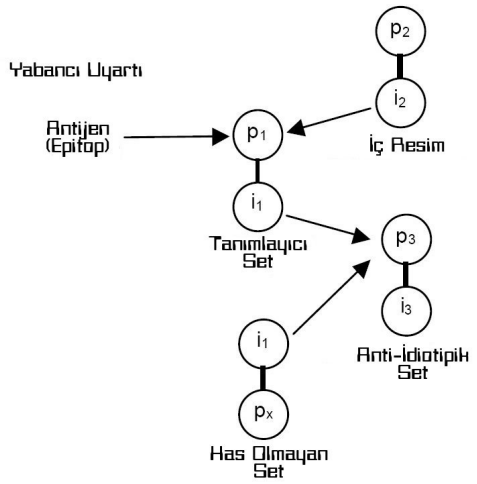
Paratop : Antikor moleküllerinin antijenleri tanımaya yönelik olan bölgeleri.

Epitop : Antijenler üzerinde bulunan tanımlayıcı bölge.

İdiotop : Antikor moleküllerinin üzerinde bulunan Epitoplar.

İdiotip : Bir Antikor seti üzerinde bulunan Epitop seti. (İdiotop Seti)

Bu noktada, idiotopların varlığının deneysel olarak tespit edilmiş olduğunu belirtelim. İdiotop örüntüleri, antikorların üzerinde paratopların bulunduğu aynı değişken bölge (polipeptid zincir) üzerinde bulunur. Bunlara dayanarak, bağışıklık sisteminin, birbirini tanıyan idiotop ve paratop setlerinin oluşturduğu son derece büyük ve karmaşık bir devre olduğu tanımı yapılmıştır. Bu durumda, devreyi oluşturan her bileşen, diğerlerini tanır ve diğerleri tarafından tanınır diyebiliriz. Antijenlere duyarlı lenfositler tanımlama sinyaline pozitif veya negatif tepki verebilirler. Pozitif bir tepki lenfositlerin çoğalmasına ve etkinleşerek antikor salgılamaya başlamalarına sebep olurken, negatif bir sinyal toleransa ye atıllığa sebep olur.



Bağışıklık sistemi bir (Ag) antijenine maruz kaldığı zaman, Ag'nin epitopu bağışıklık devresindeki bir paratop setince tanınır (bu tanıma kısmen veya tamamen olabilir). Bu paratoplar antikor moleküleri ve almaç moleküller üzerinde, P_1 paratop seti ve $İ_1$ idiotop seti eşleşebilecek şekilde birlikte bulunur. P_1 $İ_1$ sembolü, toplam tanımlayıcı antikor moleküllerini ve (Ag) üzerindeki bu tanımlamaya cevap verebilecek lenfositleri temsil eder. Bağışıklık Ağında, P_1 setindeki her paratop, bir idiotop setini tanır. Bu sayede P_1 seti çok daha geniş bir idiotop yelpazesini tanıyabilir. Son sözünü ettiğimiz idiotop setine $İ_2$ dersek, bu set, (Ag) epitopunun iç resmi olur; çünkü (Ag) antijenine ait epitop da aynı P_1 setiyle tanımlanır. Son sözünü ettiğimiz $İ_2$ idiotop seti, hücre duvarlarındaki almaçlarda ve yine tanımlayıcı moleküllerde bulunan P_2 paratop setince de tanınır. Dahası, P_1 $İ_1$ setinin her idiotopu P_1

den farklı bir P_3 paratop setince tanınır. P_3 paratop seti $İ_1$ den farklı olarak antikor ve lenfositler üzerindeki $İ_3$ anti-idiotipik seti de tanır. Bu çekirdek düzeni takip ederek, bağışıklık devresi içinde önceden tanımlanmış, birbirini tanıyan daha geniş ve karmaşık setlere ulaşabiliriz.

P_1 $İ_1$ setinin tanınmasının yanında, ona paralel P_x $İ_1$ gibi immünoglobülin ve hücre almaçları seti de bulunur. Bunlar üzerlerinde $İ_1$ idiotopları ve diğer bileşenlerle etkileşmeyen P_x paratoplarını bulundururlar. P_x paratopu bir antijen epitopuyla eşleştiğinde bir etkileşme başlarken; $İ_1$ idiotopu hücre duvarları veya bağışıklık devresini oluşturan bileşenlerden biri tarafından tanımlandığında tepkisizliğe sebep olur. Buraya kadar ifade ettiğimiz fikirler bağışıklık sisteminin kendine has olanı veya olmayanı belirleme yöntemini betimler.

Özet olarak, Yapay-Bağışık Devre kuramının çekirdek özelliği, kişinin moleküler kimliğinin belirlenmesidir.

Yapay-Bağışık Devreler kuramı, her ne kadar omurgalıların bağışıklık sisteminden esinlenilerek ortaya atılmış olsa da, uygulama alanları sadece güvenliğe ilişkin değildir. Ağ ve İletişim güvenliği üzerine uygulamalar olmasının yanında; bildik hesaplama yöntemleri kullanılarak etkin bir şekilde çözülemeyen pek çok probleme de uyarlanmaya çalışılmıştır.

Yapılan çalışmalar arasında, örüntü tanımlama, uyarlamalı sentez, tanı ve kontrol sistemleri, optimizasyon, virüs tanımlama, genetik programlama, veri işleme ve sınıflama gibi örnekler de bulunur.

Bu örneklerin gerçeklenmesinde yüksek derecede matematiksel soyutlamalara ve genellemeler kullanılır. İlginç örneklerden biri, bir veya birkaç robotun hiçbir dış yönlendirme almadan, kendi başına kararlar vererek yolunu bulmasını sağlamaya yönelik olan çalışmadır. Robottan beklenen, etrafta rastgele dağılmış olan çöpleri toplayıp çöp kutusuna atmasıdır. Bu problemde engeller, çöplerin varlığının tespiti, güç kaynağında kalan enerji miktarı ve çöp kutusunun yeri değişik antijenler olarak soyutlanmıştır. Robota yüklenmiş olan Yapay-Bağışık Devre algoritmalarının robotun istenen davranışı göstermesini sağlamasına çalışılmıştır.

Önceki örnekten de anlaşılabileceği gibi, güvenlik amaçlı kurulmuş olan omurgalı bağışıklık sisteminin, matematiksel soyutlamalar ve genellemeler yardımıyla, çok daha değişik problemlerin çözümü için kullanılabilmesi mümkün olabilmektedir.

3.2) Saldırı-Bağışık Ağlar

Bağışıklık sistemi, son derece karmaşık bir sistem olmasıyla birlikte, tam olarak bulaşıcı hastalıkların tespiti ve yok edilmesi için optimize edilmiş bir yapı sergilemektedir. Ayrıca dağıtık veri-işleme konusunda oldukça tatminkar bir örnektir; kendi kendini uyarlayabilen sistemler geliştirmek yönünde de incelenebilir.

Kendi kedini uyarlama konusundaki en önemli ve doğal olarak öne çıkan örneklerden biri bilgisayar ve ağ güvenliğidir. Bir Ağ güvenlik sistemi, bir veya daha çok makinayı izinsiz erişim hakkı almaya çalışanlardan veya yabancı kodlardan korumalıdır. Bu bağlamda, bir saldırı bağışık ağın yapması beklenen iş, bağışıklık sisteminin omurgalılar için yaptığı, bedeni koruma, ve istilacıları dışarıda tutma işinin benzeridir.

Bu tür bir sistem tasarlamada bağışıklık sisteminden öğrendiğimiz bazı fikirlere sıkı sıkıya bağlanırız:

- Bağışıklık sistemi *çok çeşitlilik* gösteren bir istemdir bu da sağlamlığını kişi ve toplum bazında artırır.
- Bağışıklık sistemi *dağıtık* bir yapıdadır. Sistem, genel bir koruma sağlamak üzere birbiriyle yerel etkileşim içinde olan pek çok bileşen barındırır. Tek merkezli kontrolü yoktur.
- *Hata Toleransı* yüksektir. Sınıflama işlerince veya verilen bir yanlış bir tepki sebebiyle oluşabilecek hatalar karşısında kolayca yıkılmaz.
- *Devinimli* bir sistemdir. Sistemi oluşturan her parçanın bir yaşam süresi vardır. Bu süre dolduğunda veya parça her hangi bir dış etken sebebiyle yok edildiğinde, parçalar yeniden yaratılırlar ve beden içinde dolaşıma katılırlar. Bu uzaysal çeşitlenmeyi artırıcı bir etkendir. Bu sayede sistem neyin zararlı, tehlikeli veya işe yaramaz olduğunu tespit eder.
- *Kendi kendini korur.* Bedeni koruyan mekanizmalar aynı amanda bağışıklık sistemini de zararlılara karşı korur.
- Kendi kendini ortam şartlarına *uyarlayabilir.*
- *Bellek ve Öğrenme* yetisi vardır. Daha önce karşılaşmadığı saldırganları tespit edip, tepki verebilir ve bunu karşılaşmalardan elde ettiği bilgiyi ileride daha hızlı tepki vermek üzere belleğine saklayabilir.

Daha önce de bahsedildiği gibi, bağışıklık sisteminin ana elemanları lenfositlerdir. Lenfositler kabaca B ve T hücreleri olarak ikiye ayrılırlar. B lenfositler, saldırıya tanı koyma, saldırı geçmişi

hatırlama antikor salgılama ve Tanıya göre T lenfositleri tetikleme işlerini yaparlar. T lenfositler tehdit oluşturan zararlılara saldırıp sindirirler. Bu işlerde antijenler baş roldedir. Antijenler sayesinde her bileşenin ve zararlının kimliği tespit edilebilir. Bir saldırı karşısında iki tür tepki verilir:

- Birincil tepki, doğuştan gelen bağışıklık bilgisi kullanılarak hiç karşılaşılmamış bir antijene karşı verilir. Ortamdaki antijene özel B lenfositler pek çok yeni antikor üretirler. Antikorlar antijenlere kabaca anahtar-kilit mekanizmasına benzer bir şekilde bağlanırlar. Bağlanan antijenler yok edilecek zararlıyı (patojeni) T lenfositler için işaretlemiş olur.
- İkincil tepki ise, daha önce karşılaşılmış bir patojenle (öncekinin tıpatıp aynısı olmak zorunda değildir.) yeniden karşılaşılmasıyla verilen bellek güdümlü tepkidir. Bu bellek yapısı ve kullandığı süreçler, *uyarlamalı bellek* (adaptive memory) süreci konusunda yapılan tartışmaların ana odağını oluşturmaktadır.

Pek çok model, bağışıklık sisteminin nasıl tepki verdiğini açıklamaya çalışmaktadır ama bu işi tam olarak yapabilen bir teori yoktur. Ayrı ayrı kuramlar ortaya atılmıştır ve bunların bazıları (haslık belirlenimi ve tehlike kuram gibi) birbirleriyle çelişir durumdadırlar. Şimdi bu kuramlara kısaca değinelim.

3.2.1) Saldırı Bağışık Ağlara İlişkin Kuramlar

3.2.1.1) Seçimsel İkizleme

Bir bağışıklık tepkisi verildiğinde, lenfositler çoğalmaları yönünde uyarılırlar ve uyaran antijene karşı antikorlarını serbestlerler. Bu çoğalma işlemi sırasında yeni oluşan B lenfositlerde bazı mutasyonlar gerçekleşir. Bu mutasyonlar, “somatik hipermutasyonlar” olarak adlandırılırlar. Amaçları ise hedef alınan antijeni hata iyi tespit edebilmektir. Hangi B lenfositler hedef alınan antijene bağlanmaya daha çok eğilim gösteriyorlarsa o tür daha çok üretilmeye başlanır. Bu sürece bağışıklık olgunlaşması süreci (Immunity maturation process [Leandro, Nunes, de Castro 200]) denir. Bu süreç bağışıklık sistemin öğrenme mekanizmalarından biridir. Yüksek bağlanma eğilimi gösteren B lenfositler uzun yaşam döngüsü olan bellek hücrelerine dönüşür ve kendilerini ikizlerler. Bu bellek hücreler sayesinde önceki karşılaşmalardan öğrenilenlerin ileri tarihteki ikinci bir karşılaşmada kullanılması ve bağışıklık sisteminin daha hızlı tepki vermesi mümkün olabilmektedir. Bu seçimsel ikizleme işlemi, bağışıklık sistemi içindeki patojene-özel bir cevabın çoğalmasını ve bellekte tutulmasını evrimsel bir algoritma çerçevesinde kısmen açıklasa da hala antijenlerin nasıl tanındığı konusunda açık noktalar olduğu bilinmektedir. Özellikle de bedene giren her yabancı antijenin (örneğin yiyecekler) zararlı çerçevesinde görülemeyeceği açıktır. Bağışıklık sisteminin bu ayrıma nası vardığı halen tartışma konusudur.

3.2.1.2) Haslık Belirlenimi

Bağışıklık sisteminin kendi ne has olan antijenlerini ayırt etmesi son dece önemlidir. Aksi bir durumda bağışıklık sistemi vücudun kendi hücrelerini de zararlı olarak algılayacaktır. Bu konu hala çekişmeli tartışmalara sebep olmaktadır. Bunun için günümüzde sıklıkla kullanılan "T-lenfositlerin timüssel negatif seçimi" (tymic negative selection of T-cells) deneysel yollarla ortaya atılmıştır [Leandro Nunes de Castro 2003].

Buna göre gelişimini tamamlamış T-lenfositler, ancak bağışıklık sistemini oluşturan antijenlere karşı eğilimi yoksa kana verilmektedir. Aksi takdirde timüs bezinde geri dönüştürülürler. Bu sayede T-lenfositlerin tanı kümesi kendi dışındaki uzaya indirgenmiş olur. Fakat bu da yeterli değildir. Daha önce belirttiğimiz gibi bu davranış sistemin su, yemek, mide bakterisi gibi yabancılara tepki vermemesini açıklamaz. Bu noktada devreye tehlike teorisi girer.

3.2.1.3) Tehlike Teorisi

Buna göre bağışıklık sistemi sadece patojenlere tepki verir. Sadece has olmama durumu bir tepki verilmesini sağlamaz. Kısaca tehlike teorisini Brectscher-Cohn iki-sinyal modeline göre ifade edelim. Bu modelde iki tür sinyal vardır. Birincisi antijen tanımlama sinyali, ikincisi yardımcı-uyartısı (co-stimulation) sinyali olarak tanımlanır. Yardımcı-uyartı sinyali "bu antijen gerçekten yabancı" veya başka bir deyişle "bu antijen gerçekten tehlikeli!" anlamına gelir. Sinyallerin oluşum şeklini bir kenara bırakıp lenfositlerin davranışlarına olan etkilerini incelemeye çalışırsak, aşağıdaki üç yasayı yazarız:

Yasa 1: 1. ve 2. sinyali alırsan etkinleş. Eğer sinyal 1'i alır 2'yi almazsan tepki verme. Sinyal 2'yi sinyal 1 gelmeden kabul etme.

Yasa 2: Sinyal 2'yi sadece antijen-tanıtıcı hücrelerden kabul et. Sinyal 1 herhangi bir hücreden gelebilir.

Yasa 3: Etkinleşme sonrasında, kısa bir sürede atıl duruma dön. (Bu sayede T-lenfositlerin kapsama alanı daralır.)

3.2.2) Ağ Güvenliğine Yönelik bir Uygulama Örneği

Şimdi, Bu konuda yazılmış makalelerden birini inceleyelim: "Extending the Computer Defense Immune System: Network Intrusion Detection with A Multiobjective Evolutionary Programming Aapproach." [Kevin P. Anchor, Jesse B. Zydallis, Gregg H. Gunch, Gary B. Lamount]

Makalenin yazarları, sonlu durum çevirgeçlerinden (Finite State Transducers) oluşan antikorları, bir evrimleştirme algoritması ile evrimleştirip sistemi aşılama yoluna gitmişler. Deneysel sonuçların saldırı ve sızma tespiti konusunda tatminkar olduğu sonucuna varmışlar.

3.2.2.1) Kullanılan Algoritmalar

- *Anormallik Tesipiti:* Bir sistemin normal davranışı, bir zaman dilimi içinde değişik aralıklarla alınan ölçümlerle tanımlanabilir. Yenilikleri veya anormallikleri tespit etme meselesi sistemin önceden tespit edilmiş normal davranış karakteristiğinden yaptığı sapmalar göz önüne alınarak çözümlenmeye çalışılır.

- *İmza tabanlı tespit:* Bu yöntemde olası bilinen saldırılara karşı bir veri tabanı vardır. Veri tabanına uymayan veri imzaları tehlikesiz sayılır ve geçmesine izin verilir.

- *Evrimsel Programlama:* Çok genel olarak bakıldığında evrimsel programlama çeşitleri birbirlerine benzer yapıdadırlar çünkü hepsi biyolojik algoritma olarak biyolojik süreçleri modellemeye çalışırlar. Yine de bu algoritmaları, *türetme* ve *seçim* süreçleri algoritmaları olarak ikiye ayırabiliriz. Standart bir evrimsel program algoritması, rastgele belirlediği bir birey kümesinden yola çıkar. Bu yaklaşımın, *arama uzayında* ki çözümlerden büyük bir kısmını örneklemesi beklenir. Bir kere başlangıç kümesi seçildikten sonra, tüm küme elemanları bir uyuşum (fitness) fonksiyonuyla değerlendirilir. Bu fonksiyonun verdiği değerler daha sonra seçim/karar verme operatörü tarafından kullanılacaktır. Tüm küme elemanlarına bir mutasyon operatörü de uygulanır. Bu operatör, küme elemanlarının arama uzayında yer değiştirmesini ve olası başka çözüm kombinasyonlarını oluşturmasını sağlar. Bunu kısaca, evrimsel programın eniyi sonucu arama süreci olarak tanımlayabiliriz. Her yeni mutasyondan sonra uyuşum fonksiyonu yeni küme üyelerine uygulanıp bir sonraki nesil elemanların hangileri olacağına karar verilmeye çalışılır. Algoritma belli bir kritere erişince durur.

- *Çok Hedefli Evrimsel Programlama (Multi-Objective Evolutionary Algorithm):* Bu öncekine göre daha yeni algoritmalar içeren bir programlama şeklidir. Gerçek problemlere uygulanabilirliği açısından pek çok bilimcinin ilgisini çekmektedir. Bu yapıyı anlamak için öncelikle bazı tanımlamalar yapmak gerekir. Bir fonksiyon için genel

maksimum veya genel minimum bulma işine “Global Optimizasyon” denir.

- Pareto Optimizasyonu, birbirine bağlı “hedef tanımlayıcı” fonksiyonların, seçilen bir “harcama” kriterine göre minimize edilmesidir. Örneğin bir kişi, bir mesafeyi en kısa zamanda, ve minimum para harcamasıyla aşmak istiyorsa, ya paradan ya da zamandan ödün vermek zorundadır. Çünkü bu “hedeflere” ait fonksiyonlar birbirlerine bağımlıdır. İstenen hedefe ulaşmak için *n* tane fonksiyon içinden bir kısmının seçili “hedef” kritere göre maksimize edilmesi diğer bir kısmın ise minimize edilmesi gerekebilir. Bazı çözümü olmayan durumlarda maksimize ve minimize edilmiş fonksiyonların bir kombinasyonu da kullanılabilir. Pareto Optimizasyonu bir hedef fonksiyona ait vektörün bir boyutunda en iyi sunuca ulaşırsa, en azından diğer bir boyutta kötüleşmeye sebep olacaktır. Arzu edilen sonuç, diğer boyutlarda minimum optimizasyon kaybı sağlamaktır. Bu durum, Karar verme mekanizmasını Pareto sonuçlarından, içinde bulunduğu duruma göre, diğer boyutlardan ödün vererek bir seçim yapmaya zorlar.

Bu tanımlamalardan sonra, genel olarak yapıyı ele alırsak, üç farklı yaklaşımla karşılaşırız: Birikme Yaklaşımı (Aggregation), Nüfus tabanlı Pareto olmayan yaklaşım, Pareto tabanlı yaklaşımı. İncelediğimiz çalışmada, ilk iki yaklaşım karar verme mekanizmasında kullanılmış. Buna göre her küme bireyine (Burada “Sonlu durum çevirgeçi” oluyorlar) uygulanan “uyuşum fonksiyonunun” verdiği değerlere göre sonuçlar öncelik açısından sıraya konuyor (Nüfus Tabanlı yaklaşım).

3.2.2.2) İzinsiz Erişim Tespiti

İzinsiz erişim tespiti için ana bileşen olarak sonlu durum çevirgeçleri (SDÇ) seçilmiş. Burada SDÇ, omurgalı bağışıklık sistemindeki antikorların karşılığı olarak düşünülmüş. Her SDÇ girdi olarak bir ağ paketi dizisi alıp; çıktı olarak “Saldırı” (D) veya “Saldırı Değil” (N) gibi bir cevap verecek şekilde tasarlanmış. Bir paket dizisinin, saldırı olup olmadığını anlamak için IP ve TCP başlığı içinde bulunan bilgiler ve buna bağlı olarak, bu bilgiler arasındaki ilintilerin incelenmesi sağlanmış. Yani, alışıla gelmiş “alev duvarı” kuralları yerine, paketler arasındaki adres ilintilerinden yola çıkarak ağdaki normal-dışı davranışın tespit edilmesine çalışılmış. Kullanılan paketler arası ilişkiler aşağıdaki gibi verilmiş:

IP Başlığı Ilintileri	TCP'ye Ozgü Ilintiler
Aynı-IP-Class-A-Src	Aynı-TCP-Port-Src
Aynı-IP-Class-B-Src	Aynı-TCP-Port-Dest
Aynı-IP-Class-C-Src	Aynı-TCP-Flags
Aynı-IP-Class-D-Src	Aynı-TCP-Seq-Num
Aynı-IP-Class-A-Dest	Aynı-TCP-Next-Seq-Num
Aynı-IP-Class-B-Dest	Aynı-TCP-Ack-Number
Aynı-IP-Class-C-Dest	Aynı-TCP-Size
Aynı-IP-Class-D-Dest	
Aynı-IP-Flags	
Aynı-Packet-Len	
Aynı-IP-ID-Num	
Aynı-IP-TTL	

Alan Ismi	Alabildiği Değerler
IP Alanları	**(Tüm paketler)**
IP Ident. Number	0-65535
IP Time to live (TTL)	0-255
IP Flags	0-65535
IP Overall Packet Length	0-65535
IP Source Address	Geçerli IP adresi
IP Dest. Address	Geçerli IP adresi
TCP'ye Ozgü Alanlar	**(Yalnızca TCP Paketleri)**
TCP Source Port	0-65535
TCP Dest. Port	0-65535
TCP Seq. Num	0-4294967295
TCP Ack Num	0-4294967295
Tek TCP Bayrakları	
(PCWR, Echo, Urgent, Ack, Push, Reset, Syn, Fin)	Boolean

Burada bir diğer nokta, paketlerin bilgi içeriği, göz önünde bulundurulmamış olması. Bunun temel sebebi arama uzayını çok büyütmesi ve ciddi miktarda işlem gücü istemesi olarak gösterilmiş. Ayrıca, bu iş için imza tabanlı çalışan tarayıcıların zaten tasarlanmış olduğunu da göz önünde bulundurmak gerekir.

Sistem ilk başlatıldığında, rastgele durumlarda SDÇ'ler üretiyor. Tüm SDÇ'ler kendi içlerinde paketler arası ilintilere dayalı bir bilgi taşıyor. İşte bu bilgi, omurgalı bağışıklık sistemindeki gen kodlarına karşılık geliyor (genotip). SDÇ'nin verdiği N veya D çıktısı ise biyolojik sistemlerdeki fenotip (Son fiziksel görünüm) kavramına denk geliyor.

SDÇ'lerin işleme süreci, ağ üzerinden gelen işaretlerin, bu SDÇ'lere girdi olarak verilip, verilmesiyle başlıyor. SDÇ'ler kendilerine gelen paket dizileri arasındaki ilintileri kendi bilgileriyle (genomlarıyla) işleyip bir çıktı veriyorlar. Bu çıktılar, uyuşum fonksiyonu tarafından değerlendirilip "0 ≥ Çıktı ≥ 1" gibi değerlerden biri atanıyor. D sinyali burada uyuşum fonksiyonunun "1" çıktısına denk geliyor. Eğer SDÇ, bir saldırı örüntüsü tespit edebilmiş görünüyorsa, diğer bir uyuşum fonksiyonu, sisteme "has" olan paket dizileriyle, söz konusu SDÇ'yi ikinci bir teste tabi tutuyor. Eğer SDÇ bu paket dizilerine de "D" sinyali veriyorsa, bir ceza puanı alıp mutasyon operatörüne gönderiliyor. En başta uyuşum fonksiyonundan 1'den küçük bir değer alanlar yine mutasyon operatörüne gönderiliyorlar.

Bu noktada, mutasyon ve rastgele süreçlerle ilgili bir iki noktaya değinelim: Daha önce de bahsettiğimiz gibi biyolojik sistemlerde iki tür rastgele sürç vardı; biri rekombinasyon, diğeri somatik hipermutasyondu. İncelediğimiz bu çalışmada kullanılan mutasyon operatörü sadece somatik hipermutasyon türü bir değişiklikte bulunuyor. Yani SDÇ'ler içindeki ilintilere yenileri eklemek, çıkarmak; başlangıç durumunu değiştirmek, çıkış işaretini değiştirmek, durumlar arasındaki geçişi değiştirmek gibi işler yapıyor. Bu işler, bazı kurallarla (ör. İçinde tek bir ilinti bulunan SDÇ'den silme yapılmaması) sınırlandırılmış rastgele süreçlerle gerçekleştiriliyor. Tüm bu mutasyon ve değerlendirme işlemleri "arama uzayı" içindeki "saldırı örüntüleri" şeklindeki çözümlere yaklaşabilmek adına yapılıyor.

Mutasyon operatörlerinden geçirilerek üretilen ikinci nesil SDÇ'ler tekrardan ağdan gelen paket dizilerine ve uyuşum fonksiyonlarına tabi tutulup değerlendiriliyorlar. Kullanıcı tarafından belirlenen bir kritere ulaşıldığında bu süreç durduruluyor.

İncelediğimiz bu yayında, kullanılan "pareto-tabanlı olmayan" yaklaşım yerine, pareto-tabanlı bir yaklaşım da oturtulabilirdi. Böyle bir yapının neye benzeyeceğine kısaca değinelim: Bunun için farklı hedefler güden "uyuşum fonksiyonları" yaratılıp bu uyuşum fonksiyonlarının SDÇ'lerden

aldıkları çıktılara verdikleri değerler göz önünde tutulur. Bu durumda, ana hedef ve ikincil hedefler kullanıcı tarafından sisteme girilmelidir. Bu verilere göre değerlendirilen çıktılar, aynı hedef için arama uzayındaki hedeflere ait sayılamayacak kadar çok optimum çözüm üretebilir. Bu çözümler basitçe, "hedef uzayındaki" hedef vektörünün başat (non-dominated) bileşenlerinin değişik kombinasyoları olabilir. Yani hedefe uygun optimum çözümler, değişik ikincil hedeflerden ödün verilerek yaratılabilirler. Buna göre, karşılaştırmaya giren SDÇ setinden, bir alt-set seçilip evrimleştirme sürecinin diğer adımlara devam edilebilir. Kişisel fikrim, pareto tabanlı karar verme mekanizmasının, yarattığı çözümlerin çokluğu sebebiyle, ciddi miktarda bellek ve işlem gücü isteyeceği yönündedir.

4) DÜŞÜNCELER...

Daha önce de söylediğimiz gibi, yapay-bağışık devreler ve uygulamaları, matematiksel genellemeler ve soyutlamalar göz önüne alındığında son derece geniş bir araştırma ve uygulama alanı yaratıyor. Yeni gelişmekte olan bir alan olması ve vaat ettiği yetenekler pek çok araştırmacıyı bu alanda çalışma yönüne çekmiş görünüyor.

Bu konudaki kişisel düşüncem, doğal sistemlerdeki optimize ve kararlı sistemlerin keşfi ve modellenmesi çabalarının, non-lineer problemler karşısında cılız kalan lineer yöntemleri geride bırakacak yeni çözümleri getireceği yönündedir. Bizim güncel olarak kullandığımız yöntemlerdeki tek merkezliliğin ve çeşitsizliğin, zaten doğanın evrimi ve yapısı ile tezat oluşturduğunu düşünüyorum. Eğer doğanın davranışlarını öngörmek ve başka problemleri çözmek için taklit etmek istiyorsak, düşüncelerimizi lineer fikirlerin yarattığı tembellikten kurtarmamız ve non-lineer davranışların istatistiksel boyutuna taşımaya çalışmamız gerektiği zorunluluğunu derinden hissediyorum...

5) KAYNAKLAR:

- Leandro Nunes de Castro, Fernando José Von Zuben – Artificial Immune Sytems: Part I Basic Theory And Applications
- Leandro Nunes de Castro, Fernando José Von Zuben – Artificial Immune Sytems: Part II A Survey of Applications
- Kevin P. Anchor, Jesse B. Zydallis, Gregg H. Gunsch, Gary B. Lamount – Extending the Computer Defense Immune System: Network Intrusion Detection with a Multiobjective Evolutionary Programming Approach
- Simon M. Garett – A Paratope is not an Epitope: Implications for Immune Network Models and Clonal Selection
- Stephanie Forrest, Steven A. Hofmeyr – John Hollands' Invisible Hand: An Artificial Immune System
- Anil Somayaji, Stephanie Forrest, Steven A. Hofmeyr – Principles of a Computer Immune System
- Steven A. Hofmeyr, Stephanie Forrest – Immnunity by Design: An Artificial Immune System
- Juan Carlos Galeano, Angelica Veloza-Suan, Fabio A. Gonzalez – A Comparative Analysis of Artificial Immune Network Models
- Uwe Alckelin, Steve Cayzer – The Danger Theory and Its Applicaton to Artificial Immune Systems
- Julien Franzolini, Damien Olivier – Self-Organisaion In An Artificial Immune Network System
- Leandro Nunes de Castro - The immune reponse of an Artificial Immune Network
- Leandro N. de Castro, Fernando J. Von Zuben – Immune and Neural Network Models: Theoretical and Empirical Comparisons.
- Bilmediğim irili ufaklı tanımlar için WikiPedia.