İlham Perimiz Bağışıklık Sistemi

Bilgisayarlardaki "virüs" terimini 1986 yılında ilk kez kullanan Fred Cohen, bu terimin tanımını "kendisinin yeni bir versiyonunu üreterek, başka programların içine giren ve bunları değiştiren bir program" olarak yapmıştı. Bu tanımı yaparken ilham kaynağı, saldırdıkları hücrenin kaynaklarını kullanarak kendilerini çoğaltan biyolojik virüslerdi. Bu örnekte olduğu gibi doğadaki "iyi fikirleri" çalmak, bilgisayar biliminin köklü bir geleneği. Yapay sinir ağları ve genetik algoritmalar, bu geleneğin en önemli temsilcilerinden. İlham kaynağı insan beyni olan yapay sinir ağları çalışmalarının amacı, sinir hücrelerinin insan beynindeki düzenlenişlerini modelleyerek yapay zeka geliştirmek. Genetik algoritmalarsa, doğadaki evrim mekanizmalarını taklit ederek makinelerin öğrenmesini sağlamayı hedefliyor. Şimdiye kadar kendine oldukça yaygın uygulama alanı bulan bu ikisine göre daha yeni olan bir yaklaşımsa, yapay bağışıklık sistemi.

Yapay bağışıklık sistemleri düşüncesinin doğuşunu sağlayan, bilgisayar virüslerinin ta kendisi. Siber aleme yıllarca tehdit salan bu dijital canavarlarla mücadele yolları üzerinde çalışan uzmanlar, bunu başarabilmek için türlü yöntemler denediler. Ancak bunların hiçbiri, bilgisayarlarımıza bulaşan virüslerden tamamen kurtulmamızı sağlayamadı. Son yıllardaysa bu mücadelede, biyolojik bir benzetmeye başvurarak yapay bir bağışıklık sistemi kurma çabası gündemde. İnsan vücudundaki bağışıklık sistemi, bilgisayar virüslerinin isim babalarının insan vücudunda yarattığı sorunların üstesinden başarıyla geliyor. Buradan yola çıkan uzmanlar, insan vücudunun virüslere karşı gösterdiği biyolojik savunma yöntemlerini taklit ederek bilgisayarlar üzerinde kurulacak bir bağışıklık sisteminin, tüm dünyadaki bilgisayarlardan yayılan yeni virüsleri çabucak ve otomatik olarak bulup analiz ederek, ortadan kaldırabileceğini savunuyor.

Yapay bağışıklık sistemleri alanındaki çalışmaların kökeni daha eskilere dayanıyorsa da, bu alana duyulan asıl ilgi 1996 yılında yapılan Bağışıklık Tabanlı Sistemler (Immunity Based

Systems) isimli uluslararası toplantıyla başladı. Bu toplantıdan sonra bir grup, bağışıklık sisteminin modelini çıkartarak çalışma şeklini daha iyi anlama yolunu seçti. Diğerleriyse yapay sinir ağları ve genetik algoritmalar alanlarında olduğu gibi, bağışıklık sistemini bir metafor olarak kullanma yoluna gitti. Doğadan gelen bu son metaforun en doğal uygulama alanlarıysa, finans sektöründeki ve elektronik ticaret alanındaki dolandırıcılık tespiti ve bilgisayar güvenliği oldu. Çünkü vücuttaki bağışıklık sisteminin karşılaştığı sorunlarla bilgisayar güvenliği alanında yaşanan sorunlar arasında, oldukça fazla benzerlik var. Doğal bağışıklık sistemleri canlıları bakteriler, virüsler, parazitler ve toksinler gibi tehlikeli dış patojenlerden koruyor. Bu nedenle vücuttaki rolleri, bilgisayarlardaki güvenlik sistemlerininkine benzer. Canlı organizmalarla bilgisayar sistemleri arasında birçok farklılık varsa da, benzerlikler bilgisayar güvenliğini geliştirmek için yeterince yol gösterici.

Bağışıklık Sistemimizin Marifetleri

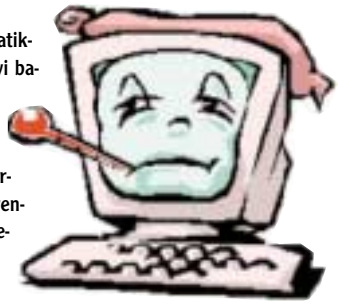
Bağışıklık sisteminin uygun bir yol gösterici model olmasının nedeni, sahip olduğu karakteristik özellikleri. Memelilerdeki bağışıklık sistemleri, yeni bilgileri öğrenebiliyor. Bunun yanı sıra, önceden öğrenilmiş bilgileri hatırlayabiliyor ve oldukça yaygın bir örüntü algılama kapasitesine sahip. Öğrenme, hatırlama, algılama ve sınıflandırma görevlerini, paralel ve adaptasyonu yüksek bir sistem kullanarak yerine getiriyor. Bu özelliği sayesinde, birbirinden bağımsız birçok farklı tehdidin üstesinden gelebiliyor. Karşılık verebildiği moleküler imza ya da antijen sayısı, 10 katrilyon. Tek bir merkezden yönetilmiyor ve hata toleransı çok yüksek. Bu da bazı hücreler fonksiyonunu yitirdiğinde ya da sistemin belli bir kısmı yok olduğunda, sistemde bir çökme yaşanmamasını sağlıyor. Ayrıca bağışıklık sistemi belli bir patojenin antijenlerini algılamayı bir kez öğrendikten sonra, bu bilgi yok olmuyor. Hücrelerden bazıları çok uzun süre hayatta kalacak "bellek" hücreleri haline geliyor ve aynı patojenin sonraki saldırılarında yeniden aktif hale geliyor. Bunların tümü, bilgisayar güvenliği bilimcilerinin oldukça işine yarayacak özellikler. Ancak, bağışıklık sisteminin iyi bir model olmasını sağlayan asıl özelliği, tüm bu fonksiyonlarının işleyiş yapısının kolayca basit algoritmalara dönüştürülebilecek nitelikte olması.

Bilgisayar güvenliği alanında halen kullanılmakta olan yöntemlerin tümü, kural tabanlı. Yani verimli olabilmeleri için, olası tüm saldırı ve tehlike türlerinin önceden tanımlanarak sisteme girilmesi gerekiyor. Bunun en önemli dezavantajı, bilgisayar alanındaki yeni bir dolandırıcılık tipinin ya da virüsün, yayılmadan önce belirlenip tanımlanmasındaki güçlük. Özellikle finans işlemlerinde sahtekarlık yapmaya çalışan kişiler, kendilerini dolandıracakları şirketin çalışanıymış gibi göstermeye kadar varan türlü yönteme başvuruyor. Vücudumuzdaki proteinleri taklit eden patojenik virüslerin davranışları da, bu kişilerinkine benzer nitelikte. Ancak memelilerin bağışıklık sistemi, barındırdığı hatırlama, genelleme ve sınıflandırma gibi özellikleri kullanarak önceden tanımadığı bu tür tehlikelere karşı da tepki verebiliyor. Bağışıklık tabanlı sistemler üzerinde çalışan uzmanların amacı, bağışıklık sistemimizin bu sorunun üstesinden gelmek için kullandığı süreçlerin benzerlerini kullanarak bilgisayar sistemlerindeki güvenlik sorunlarını çözmek.

Doğal bağışıklık sistemlerinin diğer bir önemli özelliğiyse, dışarıdan gelen saldırıları olduğu kadar, içeriden yapılan saldırıları da tespit edebiliyor olması. Bağışıklık sistemimiz bunu, vücudun kendi hücre ve moleküllerini temsil eden "kendisi" (self) ve bunların dışında kalan her şeyi kapsayan "diğerleri" (other) ayrımını yaparak başarıyor. Bu benzetmeye göre "kendisi" kavramı, bir bilgisayar sisteminin normal davranışlarına karşılık geliyor. "Diğerleri" ise önlenmek istenen ve sisteme zarar verici her tür davranışı kapsıyor. Bu yaklaşımdaki en önemli adım, bir sistemin tüm işleyişini tam olarak karakterize edecek "kendisi"nin doğru ve uygun bir tanımının yapılarak, normal dışı davranışlardan ayırt edilebilmesini sağlamak. "Diğeri", kayıtlı olmayan bir kullanıcı, bilgisayar virüsü ya da sorunlu bir veri olabilir. Sözü edilen ayrımın yapılması başarılabilirse, bir bilgisayar sistemini korumak, basit bir "kendisi" ve "diğeri" ayrımını yapma problemine dönüşecek.

Doğal bağışıklık sistemleri iki farklı tür lenfosit hücresi içeriyor; T ve B hücreleri. Bu iki hücre tipi vücudumuzda dolaşarak ve birbirleriyle etkileşerek, bağışıklık tepkilerimizi sağlıyor. Aslında bağışıklık sistemimizde birçok farklı hücre tipi daha var ve bunlar da saldırılara tepki vermemize yardımcı oluyor. Ancak bağışıklık tabanlı modellerde en sıklıkla kullanılanlar, T ve B hücreleri. Makine öğrenmesi alanındaki uzmanlarsa, özellikle B hücreleri üzerinde yoğunlaşıyor. Çünkü doğal bağışıklık sisteminin belleğinin çoğunu, B hücreleri barındırıyor. İnsan vücudunda patojenlere karşı gösterilen tepki, gitgide artan bir yapıya sahip. Bu da B hücrelerinin kendi aralarında bağlı olmasının ve bir B hücresinin patojenlere karşı uyarılma düzeyinin, bağlı olduğu diğer tüm B hücrelerinin uyarılma düzeyini etkilemesinin sonucu. Bilgisayar bilimciler, sınırlı kaynak yaklaşımı (resource limited approach) olarak ad-

landırılan bu etkileşimleri, matematiksel bağıntılar şeklinde ifade etmeyi başarmış durumdular. Şimdi üzerinde çalıştıkları alansa, bu bağıntıların bilgisayar sistemlerine uygulanması. Bunu başarabilirlerse, bilgisayarlarımıza kurulan güvenlik sistemleri, kendi kendilerini geliştirebilme özelliği kazanacak.



Bağışıklık ilhamlı tipik bir sistemde, işlemler veri zincirleri halinde temsil ediliyor. Bağışıklık sisteminin alıcılarına karşılık gelen dolandırıcılık tespit edici detektörler de, veritabanına yapılan işlem girişinin belli bir kategoriye uyup uymadığını kontrol edip karar veren bir başka veri zinciri. Normal davranışları göz ardı edip yalnızca şüpheli işlemleri yakalayacak bir sistemin, bağışıklık sisteminin rasgele genetik karıştırmayla alıcı üretmesi gibi rasgele kurallar üretebilmesi gerekiyor. Normal işlemlerce uyarılan detektörleri ayıklayabilmek için, sisteme bu detektörlerce yasal sayılan işlemlerden biri gönderilecek ve bu işlemlerden herhangi birini algılayıp tehlikeli bulan detektörler dışarıya atılacak. Normal işlemleri algılayan detektörler çıkartıldıktan sonra, kalan detektörler sistemi gözlemek amacıyla dışarıya gönderilecek. Nasıl ki bir antijen tarafından uyarılmamış lenfositler birkaç gün içinde ölüyorsa, ayarlandığı işlemle karşılaşmayan detektörler de ortadan kalkacak. Bu süreç, olasılığı daha yüksek olan dolandırıcılık tiplerinin yakalanması için geçerli kuralların daha çabuk ortaya çıkmasını sağlayacak.

Bağışıklı Bilgisayarlar Her Yerde

İnsandaki bağışıklık sisteminin bilgisayar sistemleri üzerine uygulanması çalışmaları tamamlandığında, projenin ilk uygulama alanı yasa dışı girişimlerin tespit edilmesi olacak. Geliştirilmesine 2000 yılında başlanan bu sistemin, 2003 yılında tamamlanması planlanıyor. Başlangıçta çek ve kredi kartı alanında ufak çaptaki dolandırıcılıklarla mücadele etmek için kullanılacak bu sistem başarılı olursa, Internet genelindeki tüm dolandırıcılık mücadelelerine uygulanacak. Bilgisayar Bağışıklı Dolandırıcılık Tespiti (Computational Immunology Fraud Detection-CIFD) olarak adlandırılan bu sistem, insan vücudundaki bağışıklık hücrelerinin bir bakteriyi ya da virüsü tanımasına benzer bir yol kullanarak, genel kullanım dışındaki girişimleri belirleyecek. Lenfositlerin vücuttaki normal hücreleri göz ardı etmesi gibi, CIFD sistemi de her zaman karşılaşılan rutin işlemleri göz ardı edecek. Böylece sistemin dolandırıcılık potansiyeli olan işlemleri önlemesi, daha hızlı gerçekleşecek.

Bağışıklık tabanlı sistemler başarılı olursa, kullanım alanları bilgisayarlardaki güvenlik önlemleriyle sınırlı kalmayacak. Bağışıklık sistemimiz, merkezi bir komuta birimi olmaksızın çok sayıdaki hücreyi gelişmiş tepkiler verecek şekilde koordine etme yeteneğine sahip. Bunu, hücrelerinde sakladığı proteinlerce sağlanan etkileşimler ve kimyasal sinyaller yoluyla gerçekleştiriyor. Bu özelliği nedeniyle bağışıklık sistemi, patron olmadan bir trilyon çalışanını, hiçbirine ne yapacağını söylemeksizin başarılı bir şekilde koordine eden bir iş yerine benzetilebilir. Bu özelliği bağışıklık sistemini, binlerce ya da milyonlarca robotun kumanda edilmesini gerektiren robotik projeleri için ideal bir model haline getiriyor.

Bilgisayar ve Internet üzerindeki çalışmaların hepsi gibi, bağışıklık tabanlı programlar da buraya kadar saydığımız tüm yararların yanı sıra bazı riskler barındırıyor. Bağışıklık sistemi esas alınarak geliştirilecek bilgisayar sistemleri, örüntü algılayıcı programlar geliştirmek için de kullanılacak. Bu programların kullanım amacıysa, insanların Internet üzerindeki alışveriş alışkanlıkları arasındaki ilişkileri izlemek. Internet üzerinde alışveriş yapan her bir tüketici profilinin özelliklerini listeleyebilecek bu programlar, başarılı olmaları durumunda, Internet üzerinde yapılan tüm faaliyetleri kontrol etmek için de kullanılabilecek. Bu da demek oluyor ki, bağışıklık tabanlı sistemler de kısa bir süre sonra, kendisini sanal alemdeki kontrol ve gözetleme alanındaki tartışmaların ortasında bulacak.

Ayşenur Topçuoğlu

Kaynaklar
Klarreich, E.; Inspired by Immunity; Nature, Vol. 415, 31 Ocak 2002
King, Roger L.; The Biological Basis of the Immune System as a Model for Intelligent Agents
Leyden, J.; Computer System will Sniff Out Net Fraud; www.vnunet.com
Somayaji, A.; Principles of a Computer Immune System
Dasgupta, D.; Artificial Immune Systems in Industrial Applications
Burgess, M.; Computer Immunology