

Nüfuz Tespit Sistemleri ve Mobil Ajanlar / Intrusion Detection Systems and Mobile Agents

Birol Çavuş

Gülal Sk. Detay Apt. 4/5 Cengiztopel Cad. Etiler – İstanbul
birolcavus@lba.com.tr

Özet

Başarılı bir Nüfuz tespit sistemi oluşturmak uzun bir çalışma gerektiren zor bir süreçtir ve ancak değişik teknolojilerin bir arada kullanılmasıyla mümkün olabilir. Bilgisayar güvenlik teknolojilerinin başında güvenlik duvarları, zayıflık tarayıcıları ve Nüfuz tespit sistemleri gelmektedir. IDS teknolojileri son yıllardaki yoğun çalışmalar sayesinde büyük gelişmeler göstermiştir. Ancak günümüzde, tüm sistemlerin aşmakta zorluk çektikleri bazı problemler vardır. Mobil ajan teknolojilerinin IDS'lerde kullanılmasının, Nüfuzların tespiti ve Nüfuzlara karşılık verme konularında beklenen ideal davranışa doğru gidişte büyük katkılar sağlayacağı görülmektedir. Bu yazı, mobil ajan teknolojilerinin genel olarak yazılım dünyasında sağladıkları faydaları ve IDS'ler için sağlayabilecekleri özel faydaları anlatmaktadır. Mevcut Nüfuz tespit sistemlerinin yaşadıkları sorunlar, mobil ajanların IDS'lerdeki eksikleri nasıl giderebilecekleri, Nüfuzlara karşılık vermede getirdikleri avantajlar da incelenmektedir.

1. Sunuş / Introduction

Bilgisayarların güvenliğini sağlamak, yetkili olmayan kişilerin sistemlere girip bilgileri ele geçirmelerini veya değiştirmelerini engellemek için ilk olarak doğrulama, erişim kontrolü gibi güvenlik mekanizmaları geliştirilmiştir. Bu tip mekanizmalar güvenliğin ilk basamağını oluşturmaktadır. İnternetin yaygınlaşması ile birlikte bilgi sistemlerine yönelik tehditlerde ciddi artışlar ve Nüfuzların tiplerinde genişlemeler olmaktadır. Artan tehditler nedeniyle, yukarıdaki mekanizmalar dışında yeni mekanizmaların varlığına gerek duyulmuştur. Güvenlik duvarları, zayıflık tarayıcıları ve Nüfuz tespit sistemleri güvenlik mekanizmalarının ikinci basamağını oluştururlar.

Nüfuz tespit sistemleri (IDS), bilgisayar sistemlerine, tüm tedbirlere karşın, yapılan Nüfuzları gerçekleştirirken yada gerçekleştirildikten sonra tespit etmeyi ve bu saldırılara yanıt vermeyi amaçlayan güvenlik teknolojisidir. Nüfuz tespiti için kötüye kullanım tespiti (misuse detection) ve anormallik tespiti (anomaly detection) teknikleri uygulanmaktadır. IDS'ler genelde hiyerarşik yapıya sahip sistemler olarak geliştirilmiştir. Ancak bu tip sistemlerin yaşadıkları bazı sorunlar vardır ve bunları aşmak için teknolojiye yeniliklere ihtiyaç duyulmaktadır. Bu yazı, mobil ajanların (MA) IDS sistemlerine getirecekleri yenilikler ve sorunların aşılmasında sağlayacakları faydalara odaklanmaktadır.

İlk olarak mevcut IDS sistemlerin yapıları anlatılmakta, bu yapıların karşı karşıya kaldıkları sorunlar üzerinde durulmaktadır. Mobil ajanların yazılım dünyasında çoğu durum için taşıdıkları avantajlar ve IDS sistemleri için sağlayacakları faydalar anlatılmaktadır. Ayrıca mobil ajan tabanlı olarak geliştirilmiş az sayıdaki uygulamanın özelliklerine de değinilmektedir.

2. Güvenlik sistemleri

Bilgisayar sistemlerinin güvenliğini sağlarken göz önünde bulundurulması gereken bazı özellikler vardır.

- **Erişilebilirlik (Availability):** Bilgisayar sistemi ve özellikle kritik olan bilgiler sürekli olarak yetkili kişilerin erişimine açık olmalıdır. Bilgisayar tarafından sunulan hizmete yetkili kullanıcıların erişimi engellenmemelidir. Güvenliği sağlarken bilginin erişilebilirliği kısıtlanmamalıdır.
- **Bütünlük (Integrity):** Bilgisayar sistemindeki bilgiler ve programlar belirli bir yöntemle ve yetkili olma koşuluyla değiştirilebilmelidir.
- **Doğrulama (Authenticity):** Bilgisayar sistemi kullanıcıların kimliğini doğrulayabilmeli ve kullanıcılar da bilgisayar sisteminin kimliğini doğrulayabilmelidir.
- **Gizlilik (Confidentiality):** Sistemdeki bilgiler ve transfer edilen bilgiler sadece yetkili kullanıcıların erişimine açık olmalıdır.
- **Sahip olma (Possession):** Bilgisayar sisteminin yöneticileri sistemi kontrol edebilmelidir. Kontrolün yitirilmesi, sistemde çalışmaya yetkili tüm kullanıcıları etkiler.

Güvenlikle ilgili tehditlerin sayısının ve türlerinin hızla artmasıyla birlikte, korunma teknolojilerinde de hızlı bir gelişim yaşanmaktadır. Ancak geliştirilen hiçbir teknoloji tek başına tam koruma sağlayamamaktadır. Her mekanizma belirli noktalarda koruma sunmakta, tümünün birlikte kullanımı tam bir güvenlik mekanizmasını oluşturabilmektedir. Doğrulama, erişim kontrolü, vs. gibi temel seviyedeki güvenlik mekanizmalarının dışında güvenlik için kullanılan üç teknoloji vardır [5].

- Güvenlik duvarları (firewalls)
- Nüfuz tespit sistemleri (IDS)
- Zayıflık tarayıcıları (Vulnerability scanners)

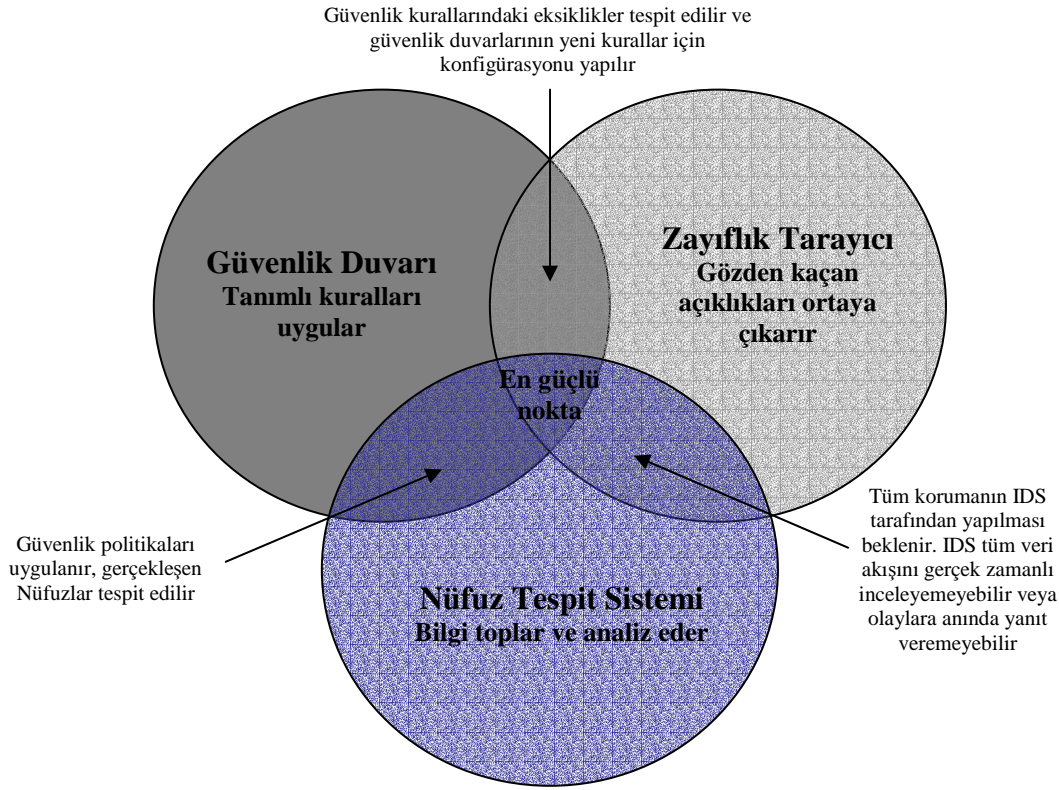
Her üç teknoloji de güvenlik açıklıklarının belirli noktalarını kapatmaktadır.

Güvenlik duvarları tanımlanmış kuralların uygulama noktalarıdır. Güvenlik duvarları ağlar arasındaki (güvenli ağlar ile güvensiz ağlar, Internet, arasına yerleştirilebilir) geçiş noktalarına yerleştirilirler ve bu farklı alanlar arasındaki bilgi geçişini kontrol ederler. Organizasyonun güvenlik politikasına göre neye izin verileceği belirlenir ve bunun dışındaki tüm bilgi akışı engellenir. Belirlenen çerçeveye göre erişim sağladıkları için olabilecek Nüfuzların çapını daraltırlar. Güvenlik duvarları iyi kada kötü olarak iki tip karar verebilirler. Şüpheye yer vermezler. Ancak saldırgan güvenlik duvarını aşmayı başardığında sistem içerisinde istediği gibi hareket edebilir. Ayrıca, yapılan araştırmalara göre Nüfuzların yaklaşık %55'i şirketlerin iç ağlarından yapılmaktadır. Bu durumda, güvenlik duvarlarının yapabileceği herhangi birşey yoktur.

Zayıflık tarayıcıları, sistemlerde Nüfuzlara maruz kalabilecek noktaları tespit etmek için kullanılırlar. Bir Nüfuz gerçekleşmeden, buna karşı önlem alınmasını sağlarlar. Zayıflık tarayıcılarının sistemde sürekli olarak çalışmalarına gerek yoktur. Tarama testleri sisteme oldukça büyük yük getirir. Testlerin belirli periyotlarda yapılması yeterlidir. Çıkan sonuçlara göre gerekli tedbirler alınır. Bu tip araçlara sadece belirli dönemlerde ihtiyaç duyulduğu, sürekli ihtiyaç duyulmadığı için bir hizmet olarak alınmaları daha doğrudur.

Nüfuz tespit sistemleri, güvenlik önlemlerinin tümünü aşmayı başarabilen Nüfuzları, gerçekleşirken yada gerçekleştikten sonra tespit etmeyi amaçlar. Hiçbir program yada güvenlik

politikası tam değildir. Her zaman programlarda hatalar olabilir yada güvenlik için tanımlanmış kurallarda eksiklikler bulunabilir. İşte bu noktada IDS'ler devreye girmektedir.



Şekil 1. Üç güvenlik teknolojisi arasındaki ilişki

Özellik	Güvenlik Duvarları	Zayıflık Tarayıcıları	Nüfuz Tespit Sistemleri
Çalışma Modu	Aktif: Kuralları uygular	Proactive: Zayıflıkları arar	Reactive: Olaylar oluştuğunda uyarılar üretir
Kontrol ettiği bilgi akışı	Güvenli ağlar arasındaki geçiş noktasına yerleştirilerek tüm trafiği gözleyebilir	Genelde Internete açık sistemleri görür	Ağ yapısına göre değişir
Hassasiyet	Kesin: Bağlantılara ya izin verilir yada verilmez	Fuzzy: Emin olmadığında uyarı verebilir	Fuzzy: Kesin Nüfuzlara yada şüpheli trafiğe göre uyarı verir
Kontrol ettiği bilgi seviyesi	Genelde alt seviye ağ trafiğini izler. Uygulama seviyesindeki trafiği de takip edebilir.	Uygulama seviyesindeki problemleri araştırır	Uygulama seviyesi için konfigüre edilebilir
Sistemlerin çalışmasına etkileri	Tüm trafik akışı üzerinden geçer. Gecikmelere neden olabilir.	Testler belirli periyodlarda çalışır ve çalışırken sistem kaynaklarını yoğun olarak kullanır	Ağ bazlı olanlar az yük getirirken, konak bazlı olanlar fazla kaynak kullanımı gerektirebilir.
Yeni Nüfuz türlerine karşı yapılması gerekenler	İzin verilen bir durumdaki eksiklikler için yeniden konfigürasyon gerekebilir.	Düzenli güncelleme gerekir.	Düzenli güncelleme ve konfigürasyon gerektirir
Kurulum karmaşıklığı	Karmaşık	Basit	Karmaşık
Bakım zorluğu	Zor	Basit	Zor
Düzenli kontrol ve analize ihtiyaçları	Gerekir	Az gerekli	Sık sık inceleme yapılmazsa bir anlamı yoktur.

Tablo 1. Güvenlik teknolojilerinin karşılaştırması

Şekil 1’de bahsedilen üç güvenlik teknolojisi arasındaki ilişki gösterilmiştir. Her teknoloji güvenlikle ilgili belirli noktalara odaklanmıştır. Hiçbiri tek başına tam güvenlik sağlayamaz. Güvenli bir sistem için her üç yapının birlikte kullanılması gerekir. Bu üç güvenlik teknolojisinin özellikleri ve karşılaştırmaları Tablo 1’de yapılmıştır.

2. Nüfuz tespit sistemleri (IDS)

“Bir kaynağın bütünlüğünü, gizliliğini, güvenilirliğini veya erişilebilirliğini engelleme amaçlı tüm davranışlar” (Heasy et al., 1990) Nüfuzun tanımını oluşturur. Daha önce de belirttiğim gibi, olabilecek tüm Nüfuzlara karşı önceden tanımlanmış kurallar oluşturarak önlem alabilmek mümkün değildir. Tüm çalışmalara rağmen, yazılım hataları ve güvenlik açıkları mutlaka olmaktadır. Bu nedenle, her zaman bilgisayar sistemlerinin Nüfuzlara maruz kalıp, istenmeyen kişilerce kullanılabilme ihtimalleri vardır. ID sistemleri, tüm mekanizmaların eksik kaldığı durumlardaki Nüfuzları tespit etmek ve ilgilileri buna karşı uyarmak için kullanılır. Nüfuz tespiti için kullanılacak, ilk akla gelen yaklaşım, log dosyalarının manual olarak incelenmesidir. Bilgisayar sistemlerindeki tüm olaylar için log bilgileri tutulmakta yani her olayın ayak izi loglarda yer almaktadır. Ancak log dosyaları oldukça fazla bilgi içerir ve manual olarak incelenmeleri çok zordur. Bu noktada, IDS’ler devreye girmektedir. ID sistemleri, bilgisayarlarda gerçekleşen aktiviteleri sürekli olarak gözlerler ve sistem güvenliğini tehlikeye sokabilecek herhangi bir olaya karşı uyarıda bulunurlar.

IDS kavramı ilk defa Anderson tarafından 1980’de ortaya konmuştur. Ancak 1987’de Denning tarafından ilk model oluşturulana kadar bir gelişim göstermemiştir. İlk ID sistemlerinde, bir konaktan toplanan veriler merkezi bir yere aktarılıyor ve burada analiz ediliyordu. Böyle bir sistem, birden fazla konağa yönelik Nüfuzları tespit etmekte zorlanacağı için ağ tabanlı sistemler geliştirilmiştir. Bu tip sistemlerde ağ paketleri incelenmektedir. Günümüzde, geliştirilen IDS’lerin büyük bir kısmı ağ tabanlıdır.

IDS’ler Nüfuz tespiti için kullandıkları yöntemlere göre iki sınıfa ayrılırlar. Nüfuz tespit yöntemleri kötüye kullanım(misuse) ve anormallik(anomaly) tespiti olarak sınıflandırılmaktadır.

- Kötüye kullanım Nüfuzları, sistemlerdeki bilinen zayıflıkları veya açıklıkları kullanırlar. Nüfuzlar, bilinen bir Nüfuz yönteminin kalıbına uyuşma ile tespit edilir. Bu bir kural tabanlı (rule-based) yaklaşımdır. Nüfuzları tespit etmek için, olabilecek Nüfuzların tümünün kalıpları çıkartılmalıdır. Kalıplara Nüfuzların imzaları (signature) denir. Bir Nüfuzun imzası olabilecek tüm varyasyonlarını çevrelemelidir. Kötüye kullanım Nüfuzlarını tespit eden bir IDS, belirli bir kalıba uymayan Nüfuzları tespit edemez.
- Anormallik durumları, sistemin normal kullanım şeklinden sapmalardır. Bu tip Nüfuzları tespit etmek için, sistemdeki tüm normal aktiviteleri içeren bir “normal profil” oluşturulmalıdır. Bu profil, kullanıcı, sistem yada her ikisi için olabilir. Normal davranış karakteristiği, klavyenin kullanımını, komut profilini yada gün içi kullanım saatlerini içerebilir. Normal profil içerisine girmeyen yada belirlenen sınırdan fazla sapma gösteren tüm aktiviteler Nüfuz olarak kabul edilir. Anormallik yaklaşımındaki sorun, eğer profilin normal olarak kabul ettiği aktiviteler çok genişse “tespit edememe (false negative)” oranı artacak, çok darsa “yanlış uyarı (false positive)” oranı artacaktır.

Tüm IDS’lerden beklenen bazı özellikler vardır [4]. Ancak bu özelliklerin bir kısmı gerçekleştirilebilir.

- Hızlı çalışma ve tüm olayları gözleyebilme (High speed, large volume monitoring)
- Ağ paketlerinin incelenmeden kaybedilmemesi (No packet filter drops)

- Gerçek zamanlı uyarıların oluşturulması (Real time notification)
- Program ve kural mekanizmasının bağımsız olması – güncelleme işlemini kolaylaştırır (Mechanism separate from policy)
- Ölçeklenebilir olma (Scalability)
- Hataya açık olmama – Kuralları tanımlarken C gibi bir dil kullanılırsa, böyle bir yapıda hata yapılması kolay olur (Avoid simple mistakes)
- Doğrudan kendisine yönelik Nüfuzlara dayanıklı olma (resistance to direct attack)

Birinci nesil IDS'ler iki katmanlı yapıya sahiptirler. Bilgi toplayıcı olarak çalışan "Collection process" loglardan ve ağdaki paketlerden bilgi topluyordu. Toplanan bilgi merkezi bir sisteme aktarılarak burada analiz ediliyordu. Analizde çeşitli yöntemler kullanılmaktaydı. Sistem büyüdükçe bu tip merkezi yapılar yeterince verimli olmamaktadır. Merkeze toplanan büyük miktardaki bilgiler bilgi-işleme sürecini uzatmakta ve zorlaştırmaktadır. İkinci nesil IDS'ler ölçeklenme problemini aşmak için çeşitli ara elemanlar ekleme yöntemini seçmişlerdir. Ara elemanlar analizden önce bilgileri ön işleme ve konsolidasyon ile ayıklama yaparlar. Bu da analiz için sadece ihtiyaç duyulan bilginin kullanılmasını sağlar.

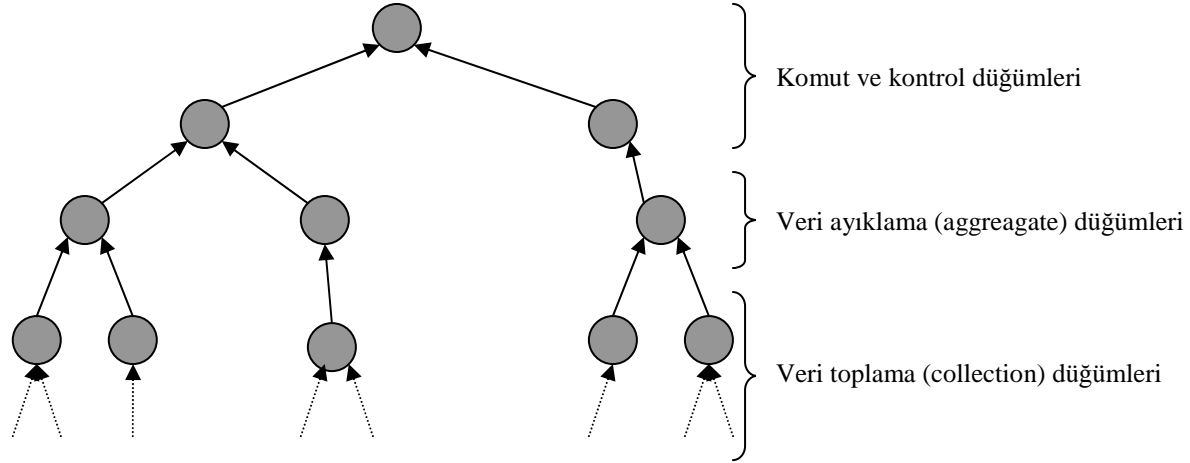
Günümüz IDS'lerinin tümü neredeyse Şekil 2'deki gibi hiyerarşik bir yapıya sahiptir. Şekil 3'te de farklı hiyerarşik yapılar gösterilmiştir [3]. Şekillerde gösterilmemekle birlikte, toplanan bilgilerin akışı hiyerarşide üst seviyelere doğru olurken, kontrol akışı genelde yukarıdan aşağıya doğru gerçekleşir. Toplanan veriler üst seviyelere aktarıldıkça bilginin özeti çıkarıldığı için genelde üst seviyelerde ihtiyaç duyulan bileşen sayısı alt seviyelerdekinden daha azdır. Bilgi toplayıcılar konumlandıkları makinalardan bilgi topladıkları için yerleri sabittir. Ancak aralardaki bileşenler girdilerini ve çıktılarını ağ bağlantıları ile alıp aktardıkları için ağ üzerinde istenilen yerde bulunabilirler. IDS'ler hiyerarşik yapıları kullanarak, ilk yöntemdeki ölçeklenebilirlik problemi aşmaktadır.

Bilgi toplama işlemi yapraklarda yapılmaktadır. Toplanan bilgiler üst seviyedeki düğümlere aggregate için aktarılırlar. Her seviyede biraz daha fazla bilgi ayıklaması olur. Merkez, Nüfuzları tespit eder ve Nüfuzlara yanıtların nasıl verileceğini belirler.

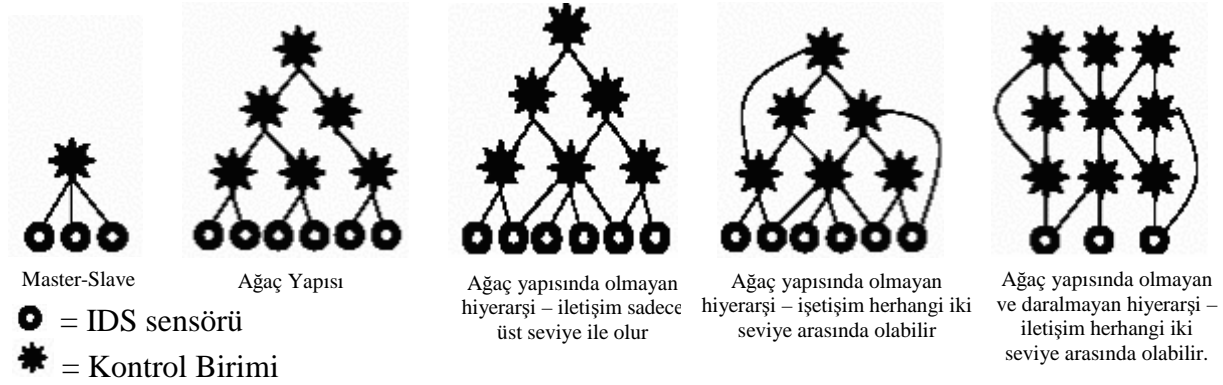
Genelde hiyerarşik sistemler verimli bir iletişim sağlar. Yapı ölçekleme için çok uygundur ancak düğümler fonksiyonları açısından birbirine çok bağlıdır ve aralarındaki bağlantının sürekli olması gerekir. Düğümler arasındaki iletişimin doğrudan doğrudan bir üst seviye ile olması şart değildir. Bazı yapılarda herhangi iki bileşen arasında iletişim olabilir. Nüfuzlara karşılık verme sürecini hızlandırmak için veri toplama elemanları kritik durumlarda doğrudan kontrol düğümüyle iletişim kurabilir.

Hiyerarşik IDS modelini kullanan sistemlere örnek olarak GrIDS, SPI-NET, Intruder Alert, RealSecure, Active Security ve Cisco tarafından geliştirilen NetRanger gibi ürünler gösterilebilir.

Hiyerarşik ID sistemleri, ölçeklenebilirlik ve organizasyonel yapıya adapte edilme konularında avantaj sağlamalarına rağmen, tasarım sırasında üzerinde önemle durulması gereken bir nokta vardır. Hiyerarşik IDS'lerde tek noktadan kaynaklanabilecek problemler nedeniyle tüm sistemin çalışması etkilenebilir ve saldırganlar bu zayıflıkları kullanabilirler. Bir saldırgan böyle bir nokta yakalayıp, burayı ele geçirirse, sistemin büyük bir kısmını devre dışı bırakıp, rahatça amaçlarına ulaşabilir.



Şekil 2. Hiyerarşik IDS yapısı



Şekil 3. Hiyerarşik IDS yapıları

IDS'ler anormallik ve kötüye kullanım tespiti için çeşitli yöntemler kullanmaktadır [2]. Tablo 2'de anormallik tespiti , Tablo 3'te ise kötüye kullanım tespiti için kullanılan yöntemler anlatılmaktadır.

Yöntem	Tanım
İstatistik	Bu yöntemde, kullanıcıların normal ve beklenen davranışları ile ilgili bilgiler, belirli bir zaman dilimi içerisinde toplanır. Daha sonra incelenen davranışlar üzerinde istatistiki testler uygulanarak davranışların doğruluğu tespit edilmeye çalışılır.
Tahmini kalıplar oluşturma (Predictive pattern generation)	Bu yöntemde, gelecekte olacak davranışlar geçmişte gerçekleşenlere göre belirlenmeye çalışılır. IDS tarafından çıkarılan kurallar bir olayın oluşma olasılığını tanımlar. Denklemin sol tarafında ardarda olabilecek iki olay, diğer tarafında bu olayların olma olasılığı bulunur. Bir olayın Nüfuz olarak nitelenebilmesi için sol taraftaki kuralın sağlanması fakat sağ tarafın beklenenden fazla sapması gerekir.
Neural Ağlar	Bu tip sistemler bir sonraki komutu belirli bir kullanıcının geçmiş komut dizilerine göre öngörebilmeyi amaçlar.
İşlem sıralarının tespiti ve öğrenilmesi (Sequence matching and learning)	Lane & Brodley anormallik tespiti için kullanılabilen bir "machine learning" uygulama geliştirmişlerdir. Bu yaklaşım bir hipotezden yola çıkmaktadır. Bir kullanıcının belirli durumlara önceden tahmin edilebilir şekilde tepki verdiğini ve bu tepkide bir dizi işlemin olduğunu kabul eder. Bir kullanıcının profilini oluşturmak için model, kullanıcı tarafından gerçekleştirilen olaylar dizisini öğrenmeye çalışır. Karakteristik hareketlerdeki değişiklik geçerli bir kullanıcı gibi görünerek gizlenmeye çalışan saldırganı tespit edebilir.

Tablo 2. Anormallik tespiti için kullanılan yaklaşımlar

Yöntem	Tanım
Uzman sistemler	Uzman sistemler geçmişteki Nüfuzlarda elde ettikleri bilgileri ve güvenlik politikasındaki kuralları inceleyerek karar verirler. Toplanan bilgileri inceleyerek karar kurallarını değerlendirirler, kurallara uyan Nüfuzları tespit ederler.
Tuş basmalarını gözleme	Kullanıcının tuş basmaları ve sistemin buna karşılık verdiği tepkileri gözlemler ve bunlardan kurallar oluşturur. Kuralların dışındaki hareketleri tespit eder.
Model tabanlı karar sistemleri	Bilinen Nüfuz türleri bir dizi davranış olarak modellenir ve bu davranışlar daha sonra log dosyalarındaki olaylara göre modellenir. Bu modellerin veritabanı oluşturur. IDS sistemdeki olayları bu veritabanındaki modellerle eşleştirmeye çalışır.
Durum geçiş analizi (state transition analysis)	Saldırganın bilgisayara Nüfuzırken gerçekleştirdiği işlemlerin grafiksel bir ifadesi olan ve bilgisayar sisteminin bu işlemler sonucundaki durumunu gösteren durum geçiş diyagramları oluşturulur. Bu analizde bir Nüfuz sistemi, bir durumdan hedeflenen duruma geçiren bir dizi olay olarak düşünülür. Durum geçiş diyagramları Nüfuzun ihtiyaçlarını ve sonucunu gösterir. Ayrıca, başarılı bir Nüfuzda atılması gereken önemli adımları gösterir.
Kalıp eşleştirme (pattern matching)	Bu modelde bilinen Nüfuzların imzalarının log bilgilerinde oluşturdukları kalıplar kullanılır. Sistemdeki aktiviteleri Nüfuz senaryolarının kalıplarına eşleştirmeye çalışır.

Tablo 3. Kötüye kullanım tespiti için kullanılan yaklaşımlar

Yöntem	A/M	Bilinen Nüfuzlar	Bililmeyen Nüfuzlar	Kendini gizleme	Denial of service	Malicious use	Leakage	Attempted brekins	Penetration of security
İstatistik	A	Evet	Evet	Evet	Hayır	Evet	Hayır	-	Hayır
Tahmini kalıplar oluşturma	A	Evet	Evet	Evet	Hayır	Evet	Hayır	-	Evet
Neural ağlar	A	Evet	Evet	Evet	Hayır	Evet	Hayır	-	Hayır
İşlem sıralarının tespiti ve öğrenilmesi	A	Evet	Evet	Evet	Hayır	Evet	Hayır	-	Hayır
Uzman sistemler	M	Evet	Hayır	Hayır	Hayır	Evet	Hayır	-	Evet
Model tabanlı	M	Evet	Hayır	Hayır	Hayır	Evet	Hayır	-	Evet
Durum geçiş analizi	M	Evet	Hayır	Hayır	Hayır	Evet	Hayır	Hayır	Evet
Kalıp eşleştirme	M	Evet	Hayır	Hayır	Hayır	Evet	Hayır	Evet	Evet

Tablo 4: Tespit edilebilecek Nüfuzlar - A/M → Anormallik / Kötüye kullanım (Misuse)

2.1. Nüfuz tespit sistemlerinin eksiklikleri

Tüm Nüfuz tespit sistemlerinde ortak olarak görülen bazı eksiklikler vardır. Teknolojideki gelişmelerle birlikte bu eksiklikler giderilmeye çalışılmaktadır.

- **Yanlış alarmların çokluğu (High Number of False Positives):** Yanlış alarmların sayısı fazla fakat Nüfuz tespiti mükemmel değildir. Yanlış alarmları azaltmak için eşik değerleri azaltılırsa tespit edilemeyen Nüfuz sayısı artar (false negatives). Nüfuzları kesin tespit etmek günümüz IDS geliştiricilerinin en temel problemidir.
- **Verimliliğin az olması (Lack of efficiency):** IDS'lerin sistemdeki aktiviteleri gerçek zamanlı değerlendirmeleri beklenir. Günümüzde çok büyük organizasyon ağları vardır ve ağlarda dolaşan bilginin büyüklüğü oldukça fazladır. Böyle büyük ağlarda bunu gerçeklemek oldukça zordur. Yapı büyüdükçe, konak bazlı sistemlerde yavaşlama görülürken, ağ tabanlı sistemlerde ağ paketleri zamanında incelenemeyerek kaybolur.

- **Bakım zorluğu (Burdensome Maintenance):** IDS'lerin bakımı ve konfigürasyonu büyük bir çalışma ve özel bir bilgi gerektirir. Örneğin, kötüye kullanım tespiti için kullanılan imzaların kural kümelerini oluşturmak ve güncellemek sistemde kullanılan özel dili ve olaylar arasındaki ilişkiyi sisteme nasıl anlatacağını bilmeyi gerektirir. Anormallik tespitinde ise istatistiki metriklerin eklenmesi gerekir.
- **Sınırlı esneklik (Limited flexibility):** IDS'ler belirli donanım ve işletim sistemlerinde çalışmak için geliştirilirler ve benzer güvenlik yapıları(policy) olan diğer ortamlarda kullanılmaları zordur.
- **Nüfuzlara açık olmaları (Vulnerability to direct attack):** IDS bileşenleri arasında hiyerarşik yapı olmasından dolayı, IDS'lerin kendileri Nüfuzlara açıktır. Saldırgan hiyerarşideki bilgi akışını bir ara elemana saldırarak kesebilir. Hatta merkeze saldırarak tüm sistemin çalışmasını engelleyebilir. Sistemin çalışması için önemli olan elemanlar, genelde doğrudan Nüfuz almayacakları yerlere yerleştirilirler.
- **Nüfuzlara karşılık vermekteki eksiklikler (Limited response capability):** IDS'ler genelde Nüfuzların tespitine odaklanmıştır. Tespit önemli olmakla birlikte, sistem yöneticisi IDS'lerden gelen raporları incelemekte ve gerekli aksiyonu almakta yeterince hızlı olmayabilir. Buda saldırgana, karşılık verilene kadar rahat kalma imkanı verir. Artık birçok IDS Nüfuzlara otomatik şekilde yanıt verecek özelliklere sahiptir ancak hala eksiklikler vardır.
- **Tasarım metodolojisi olmayışı (No generic building methodology):** Bu alanda herhangi bir metodoloji oluşmamıştır. Buda Nüfuzların tespiti için kullanılan teknikler üzerinde genel bir uzlaşma olmayışındandır.

Nüfuz tespit sistemleri bilgisayar teknolojisindeki gelişmelerle birlikte bazı yeni sorunlarla da karşı karşıya kalmaktadır. Nüfuz tespit sistemleri için yeni sayılabilecek problemler şunlardır;

- **Uçtan uca şifreleme (End-to-end encryption):** Ağda gezen bilgilerin istenmeyen kişilerden gizli tutulması için şifreleme kullanımı yaygınlaşmıştır. Bu, iletişimi dinleyenleri engellerken IDS'lerin Nüfuz tespiti için paketleri incelemelerini de zorlaştırmaktadır.
- **Yüksek hızlardaki iletişim (High Speed Communication):** Artan iletişim hızları IDS'lerin işlem gücünün artmasını gerektirmektedir. Ayrıca switched iletişime doğru yönelişin olması, ağ tabanlı bir IDS'nin birden fazla iletişimi izlemesini zorlaştırmaktadır.
- **Nüfuz türlerinin çokluğu (Breadth of attacks):** Saldırganların kullandıkları yöntemler hızla gelişmekte ve yeni Nüfuz türleri ortaya çıkmaktadır. Yeni bir Nüfuzun tespit edilebilmesi için IDS'lerin güncellenmesi gerekir. Yeni kurallar eklenirken eski kurallar atılamaz. Daha fazla Nüfuz türünü kontrol etmek için algoritmanın daha fazla işlem gücüne ihtiyacı vardır.
- **Teknolojideki sınırlamaları (Technology Limits):** Programlar veya protokoller içindeki zararlı kodları tespit etmek için program yapmak mümkün değildir. Her sistem hatalar içerir.

IDS'lere Nüfuzlar

IDS'ler doğrudan kendilerine yöneltilebilecek olan Nüfuzlara karşı korunaklı olmak zorundadırlar. IDS'lerin yetenekleri arttıkça saldırganların amaçlarına ulaşmak için ilk hedefleri, organizasyonun Nüfuz tespit sistemini etkisiz bırakmaya çalışmak olacaktır ki daha değerli hedeflere ulaşabilsinler.

3.1. Mobil ajanların sağladığı avantajlar

Mobil ajan teknolojileri mevcut bazı IDS eksikliklerini giderebilir ancak bir mucize gibi bütün eksiklikleri gidermesi beklenmemelidir. Mobil ajanların günümüz uygulamalarına sağlayacakları faydalar ve avantajları konusunda çeşitli araştırmalar yapılmaktadır. Genel olarak mobil ajanlar, klasik istemci-sunucu teknolojisine iki noktada üstünlük sağlarlar. Burada anlatılan avantajlar MA'lerin IDS'lere uygulanması durumunda da geçerlidir.

- **Esneklik (Enhanced Flexibility):** Genelde, istemciler sunucu tarafındaki kaynaklara belirli servisler ile erişirler, bu servislerin arabirimleri önceden tanımlanmış ve istemci-sunucu tarafından kabul edilmiştir. Yeni servisler oluşturmak veya mevcut servislere yeni yetenekler katmak için arabirimleri dinamik olarak değiştirmek oldukça zordur, bazen de mümkün olmayabilir. Mobil ajanlar istemci ve sunucu taraflarındaki arabirimleri dinamik olarak güncellemek için kullanılabilirler.
- **Bant genişliği kullanımının azaltılması (Reduced Bandwidth Consumption):** Mobil ajanlar normalde sunucu tarafından sağlanması gereken bazı kaynakları kendilerinde taşıyabilirler ki bu uzaktan erişim ihtiyacını azaltır, böylece iletişim ağının daha verimli kullanılması sağlanabilir.

Bu iki avantaj dışında daha birçok avantaj mevcuttur.

- **Hata toleransının artması (Improved Fault Tolerance):** Genel yapıda istemci ve sunucu arasında sürekli bir istek-cevap (request and reply) akışı vardır. Bu akışın sağlanabilmesi için her iki tarafında sürekli çalışır durumda olması gerekir. Her hangi biri sorun yaşarsa tüm sistem sorun yaşar. Mobil ajanlar kullanıldığında ise sunucu tarafından yapılması beklenen bazı işlemler mobil ajanın kodunda yer alabilir ki bu bazı işlemlerin lokal olarak yapılabilmesini sağlar.
- **Bağlantısız işlemlerin yapılabilmesi (Support for disconnected operations):** MA'ler herhangi bir sunucuya ihtiyaç duymadan bazı işlemleri gerçekleştirebilir. Bazı durumlarda bilgisayarlar iletişim imkanına sahip olmayabilirler (ör: sistem dışındaki laptoplar). Bu gibi durumlarda, mobil ajanlar bağlantısız olarak çalışmalarını sürdürebilir ve iletişim tekrar sağlandığında elde ettikleri sonuçları gerekli yerlere aktarabilir.
- **Ağ yükünün azaltılması (Reducing network load):** Verileri ağ üzerinden işlem yapılacak yere göndermekten önce mobil ajanlar verinin olduğu yere gönderilebilir, yani veri işlem yerine gideceğine işlem veriyeye gider. Böylece ağ yükü azaltılabilir.
- **Bağımsız ve asenkron çalışabilme (Autonomous and asynchronous execution):** Büyük dağıtık sistemlerde, sistemin bir kısmı zarar görürse yada çalışmaz hale gelirse sistemin geri kalanının çalışmasına devam edebilmesi önemli bir unsurdur. Mobil ajanlar yaratıldıkları bilgisayardan bağımsız olarak çalışmalarına devam edebilirler ki bu IDS elemanları için çok önemli bir özelliktir. Zarar gören elemanlar olduğunda klonlama ile zarar gören elemanlar tekrar oluşturulabilir ve fonksiyonlar geri kazanılabilir.
- **Dinamik adaptasyon (Dynamic adaption):** Mobil ajanların ortamlarındaki değişiklikleri hissedebilmeleri ve buna göre cevap verebilmeleri IDS açısından önemli bir özelliktir. Tehlikeyi önlemek için ajanlar istedikleri yere konumlanabilirler, kendilerini klonlayıp paralel işlem yapabilirler, diğer ajanlardan yardım alabilirler. Yukarıdaki özelliklerle birlikte dayanıklı ve hata toleranslı sistemler yaratılabilir.

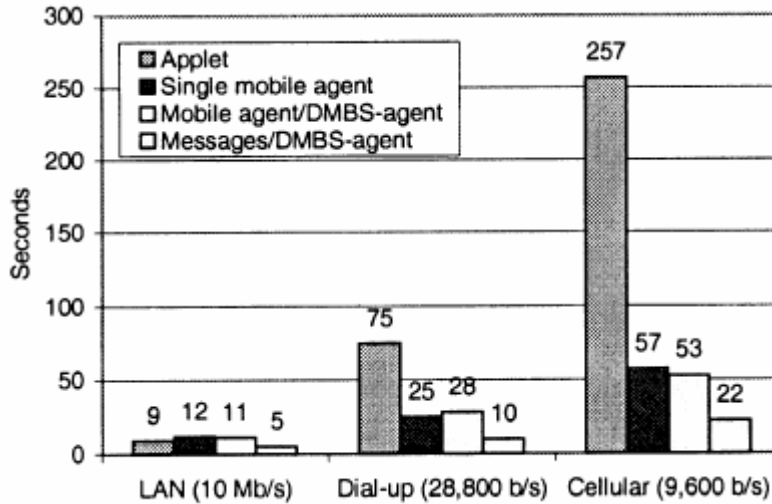
3.2. Mobil ajanların uygulama alanlarından bazıları

Mobil ajanlarla ilgilenirken en çok “mobil ajanların yapabileceği ancak geleneksel sistemlerin yapamayacağı herhangi bir iş var mıdır?” sorusu sorulur. Bu soru aslında oldukça yersizdir. Çoğu araştırmacının ortak kanaati, mobil ajanlarla sağlanabilen her türlü özelliğin geleneksel sistemler ile de sağlanabileceğidir [6]. Mobil ajan uygulamaları dağıtık sistemlerin gerçekleştirilmesi için kullanılacak bir method olarak düşünülmelidir. Nesneye yönelik programlamanın programcılıktaki yeri de böyledir. Nesneye yönelik programlama ile yapılabilen herşey klasik programlama ile de yapılabilmektedir. Ancak bir yöntem bazı alanlarda, diğeri başka alanlarda kalaylık getirir.

Aslında bazı uygulamalar mobil ajanlar için daha uygundur denebilir. Asıl önemli nokta, geleneksel sistemlerde mobil ajanlar nerelerde fayda sağlayabilir ve bu faydalar etkin bir şekilde nasıl kullanılabilir. Bu bölümde mobil ajanlarla sağlanan bazı başarılarından bahsedeceğiz.

Veritabanı erişiminde mobil ajanların kullanılması

Uzaktan veritabanı erişimlerinde, transactionların gerçekleştirilmesi ve sonuçların aktarımı noktasında mobil ajanlar kullanılabilir. Şekil 4, mobil ajanların değişik hızlardaki iletişim ortamlarında transaction gerçekleştirme sonuçlarını göstermektedir.

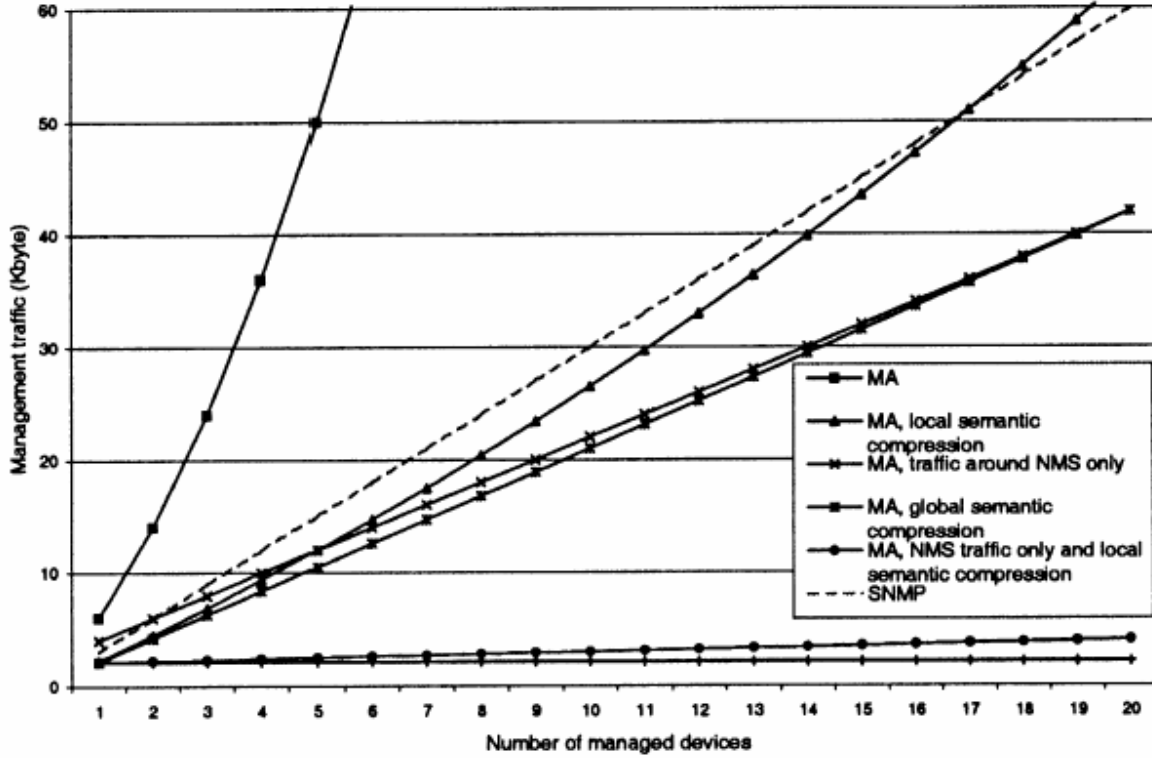


Şekil 4. Web’de küçük transactionların gerçekleştirme süreleri¹

Ağ yönetiminde mobil ajanların kullanılması

Ağ yönetiminde hala yaygın olarak kullanılan “Simple network management Protocol (SNMP)” çok merkezi bir yapıya sahiptir. Tüm ağda oluşan bilgiler tek bir merkezi noktada toplanmaktadır. Bu da bilgi aktarımında ağ trafiğinin yoğunluğunu artırır. Ağ yönetiminde mobil ajanlar kullanılarak bazı faydalar sağlanabilir. Ajanlar merkezde toplanacak bilgileri aktarım öncesinde nodelarda inceleyerek, özetler oluşturabilirler. Bu da ağ üzerindeki trafiği azaltacaktır. Şekil 5’te Baldi ve Picco tarafından hazırlanan ve mobil ajanların farklı şekillerde ağ yönetiminde kullanılmaları ile oluşan sonuçlar gösterilmiştir.

¹ Şekil 4 [6]’den alınmıştır



Şekil 5. Plain SNMP vs. Mobil ajanlar²

3.3. Mobil ajanların birlikte çalışabilmeleri için standartlar (Interoperability standards)

Ajanlar birbirleriyle iletişim için genelde üst seviye bir ajan iletişim dili (agent communication language - ACL) kullanırlar. Örnek olarak KQML gösterilebilir. Üst seviye dillerin standartlaşması ile değişik tipteki ajanların ortak bir dil üzerinden haberleşmeleri sağlanabilir. Son yıllarda böyle ortak arabirimlerin oluşturulması için üniversitelerde ve araştırma kurumlarında yoğun çalışmalar yürütülmektedir.

Günümüze kadar çeşitli mobil ajan platformları geliştirilmiş ve piyasaya sunulmuştur. Ne yazık ki bu platformlar yapıları ve tasarımları bakımından büyük farklılıklar göstermektedir ve birbirleriyle çalışma, iletişim kurma yeteneğine sahip değildir. Ancak mobil ajan platformlarının ortaklaşa çalışabilmelerini sağlamak için çeşitli standartlar geliştirilmeye de çalışılmıştır. Bu standartlar şöyledir [7];

- *MASIF (the Mobile agent system interoperability facility)*: Object management group (OMG) tarafından oluşturulmuştur. Mobil ajan platformları arasında iletişim kurulabilmesi için gerekli özellikleri belirler.
- *The knowledge query and manipulation language (KQML)*: ARPA tarafından geliştirilmiştir. Ajanlar arasında bilgi paylaşımı yapılması için kullanılacak bir dildir.
- *The FIPA specifications*: Foundation for Intelligent Physical Agents (FIPA) tarafından oluşturulmuş bir dizi standarttır. Mobil ajan teknolojileri için bir metodoloji oluşturulmuştur. Ayrıca KQML'e benzeyen bir ajan iletişim dili yaratılmıştır.

3.4. Java tabanlı mobil ajan sistemleri

² Şekil 5 [6]'dan alınmıştır.

Tüm mobil ajan sistemleri farklı donanım platformlarında çalışabilen ve kod transferinde yeniden derlemeyi gerektirmeyen, uygun yazılım sistemiyle geliştirilmelidir. Bu nedenle, iki temel kategoride mobil ajan platformları oluşturulabilir.

- Java tabanlı mobil ajan platformları (MAPs)
- Script dillerine dayanan MAP'ler

Her iki türde de çalışma zamanlı (runtime) desteğe ihtiyaç vardır, yani JVM interpreter veya script dil interpreter gerekir. Script tabanlı olan sistemlerin büyük bir kısmı Java'nın genel kabul görmesinden önce geliştirilmişlerdir. Örneğin, önemli bir MA platformu olan Odyssey sistemi Java ile tekrar implemente edilmiştir. Java tabanlı olan MAP'ler script dilerden daha kolay oluşturulabilirler. Ayrıca Java dili içerisinde mobil kod geliştirme özellikleri de vardır ve teknolojisi sürekli geliştirilmektedir. Java tabanlı MAP'lere örnek olarak aşağıdaki sistemler gösterilebilir.

- Grasshoper
- Aglets
- Concordia
- Voyager
- Odyssey

Her platform programcılarının kendi ajanlarını ve uygulamalarını geliştirmesi için gerekli sınıflara sahiptir. Bu sistemlerin tümü Java'nın nesneye yönelik programlama özelliklerini kullanır.

Ajanlar: Her platformda temel ajan davranışlarını sağlayan bir sınıf vardır. Programcılar bu sınıfı geliştirerek uygulamanın ihtiyaç duyduğu ajanı geliştirebilirler. Bazı platformlarda statik ve mobil ajanlar için tek bir sınıf, bazılarında her ikisi için de farklı sınıflar bulunur.

4. Mobil ajan tabanlı IDS'ler

Yakın gelecekte karşımıza çıkacak ID sistemlerini şu şekilde düşünebiliriz;

- Binlerce bilgi toplayıcı ajan olacaktır
- Toplanan bilgilerin analiz edildiği yüzlerce ajan olacaktır
- Özelleşmiş ajanlar kullanılacak, analiz ajanları bir veya birden fazla tip Nüfuzu tespit edebileceklerdir
- Her bilgisayarda bir veya daha fazla ajan birlikte çalışabilecektir

Mobil ajanların IDS'ler için mucize olarak görülmemeleri gerekir. IDS sistemlerinin tüm eksikliklerini MA ile gidermek mümkün değildir. Mobil ajanlar Nüfuz tespit yöntemlerinin (kötüye kullanım, anormallik tespit gibi) gelişmesini sağlamazlar. Ancak mevcut tekniklerin uygulanma biçimlerini değiştirerek, daha etkin ve başarılı çözümlerin üretilmesini sağlayabilirler. MA kullanımının IDS'in tüm bileşenleri için kullanılması etkin bir çözüm oluşturmaz. Bazı bileşenlerin statik olması uygundur. Herşeyin mobil olması sisteme çok fazla yük getirebilir. Yani mobilite sadece gereken yerlerde kullanılmalıdır [1].

Mobil ajanların ilk olarak faydalı olacakları nokta, hiyerarşik bir yapıdaki düğümler arasında transfer edilen büyük miktardaki log bilgilerinin azaltılmasını sağlamak olacaktır. Mobil ajanlar verinin bulunduğu depolara (repository) giderek buradaki bilgileri analiz (mine) edebilirler ki bu onların bilgi-işlem gücünü veriye taşıma özelliklerinin doğal sonucudur. Ağ trafiğini rahatlatmalarının yanında özelleşmiş ajanlar sayesinde belirli Nüfuzları tespit eden ajanlar yaratılabilir. Koordine olarak değişik kaynaklardan, uzun bir zaman diliminde gerçekleşen Nüfuzları tespit edebilen ajanlar geliştirilebilir.

Ağ bazlı IDS'lerden, çok sayıda ve birlikte çalışabilen ajan modeline geçildiğinde kayıp paketlerin azaltılması mümkün olacaktır. Ayrıca oluşan Nüfuzlara hızla cevap verebilme kabiliyeti artacaktır. Konaklarda sürekli olarak ajanların bulunması IDS sisteminin ağ paketlerini açık metin olarak görebilmesini sağlayacaktır (Bu IPsec gibi ağ seviyesi şifreleme uygulandığında bile mümkün olabilecektir).

Mobil ajanlar güçlü, Nüfuzlara dayanıklı IDS'lerin geliştirilmesini sağlayabilirler. Ajanlar tehlike sezdiklerinde yada kendilerine yönelik Nüfuzları tespit ettiklerinde yer değiştirebilirler, kendilerini klonlayarak çoğalabilirler, diğer ajanlarla bilgi paylaşımı yapabilirler, hatta bazı noktaları bozulmuş olan sistemi tekrar ayaklandırabilirler. Hatta akıllı ajanlar (intelligent agents) sayesinde, ajanlar öğrenme yetenekleri ile Nüfuzlara karşı daha güçlü hale gelebilirler.

Günümüz ID sistemlerinin en büyük eksiklikleri tespit edilen Nüfuzlara verilecek karşılıklarda yaşanan problemlerdir. Bu noktada, mobil ajanlar IDS'lere en büyük yararı sağlayacaktır. Nüfuzlara verilecek karşılıklar ağın herhangi bir yerinden yürütülebileceği için, mobil ajanlar Nüfuzlara verilecek karşılıklarda geleneksel IDS'lerden daha optimal sonuçlar yaratabilirler. Mobil ajanlar Nüfuznu kaynağının izini sürebilirler, Nüfuzya, hedefteki bilgisayardan yanıt verebilirler, Nüfuzya kaynağında yanıt verebilirler, Nüfuz hakkında hedeften ve diğer ağ bileşenlerinden bilgi toplayabilirler (evidence gathering), kaynak ve hedefi birbirinden ayırtabilirler. Mobil ajanların Nüfuzlara verilecek karşılıklarda sağlayacakları faydalar şu şekilde açıklanabilir;

- **Saldırganın izini sürmek (Tracing an attacker):** Saldırganlar genelde hedeflerine ulaşmak için bir dizi konak üzerinden geçerler ve bazen adreslerini gizler veya adreslerini değişik olarak gösterirler. Bu durumda, saldırganı tespit etmek için saldırganın geçtiği noktaların takip edilmesi ve paketlerin gerçekte gönderildiği yerin bulunması gerekir. Bunu yapmak için ajanın tüm ağ segmentlerini taraması ve tüm konakları analiz etmesi gerekir. Statik yapıya sahip geleneksel IDS'ler ile bunu gerçeklemek oldukça güç olmasına rağmen mobil ajanlar ile mümkündür.
- **Nüfuzya hedefte karşılık vermek (Responding at the target):** Bir Nüfuz tespit edildiğinde Nüfuzya, saydırıya maruz kalan konakta yanıt verebilmek oldukça önemlidir ve başarılırsa Nüfuzlara karşı iyi sonuçlar elde edilebilir. Hızlı yanıt verebilmek saldırganın, daha ileri noktalara gitmesini engelleyebilir ve Nüfuzsına devam etmek için ele geçirdiği konaktan faydalanmasını engellenebilir. Bu ayrıca, saldırgan tarafından yaratılan hasarın en aza indirilmesini de sağlayabilir.
- **Nüfuzya kaynakta karşılık vermek (Responding at the source):** Nüfuzlara kaynağında yanıt verebilmek IDS'ye daha fazla güç verir, böylece saldırganın hareketleri kontrol edilebilir. Mobil ajanlar olmadan, IDS'in saldırganın bilgisayarına yeterince müdahale imkanının olması mümkün değildir. Bunu mobil ajanlarla gerçekleştirmek de her durumda mümkün olmayabilir. Ajanın saldırganın bilgisayarına geçebilmesi için bilgisayarında ajanın çalışması için gerekli ortam olmalıdır. Bu da ancak saldırganın kontrol altındaki bir alanda(domain) olması ile mümkün olabilir. Bu özelliğin sağlanması IDS'ler için büyük bir gelişim anlamına gelmektedir.
- **Delil toplamak (Evidence gathering):** Geleneksel sistemlerde değişik kaynaklardan, bir Nüfuz hakkında delil toplamak mümkün değildir. Bu, doğru zamanda doğru yerde doğru programın çalıştırılmasını gerektirir. Mobil ajanlar herhangi bir programın, herhangi bir zamanda ve herhangi bir yerde çalıştırılmasını sağlama özellikleri sayesinde, değişik bilgisayarlardan, değişik işletim sistemlerinden, hatta değişik uygulamalardan (web sunucular gibi) Nüfuz hakkında delil toplanabilmesini olası kılmaktadır. Ayrıca, şüpheli yada önemli ağ noktalarındaki loglama özelliklerini gerekli durumlarda tekrar konfigüre ederek daha yoğun log işleminin yapılmasını sağlayabilirler.

- **Nüfuz kaynağı ile hedefi isole edebilmek (Isolating the source and target):** Nüfuzlara hedefte veya kaynakta karşılık vermek her zaman mümkün olmayacağı için son seçenek olarak ağ seviyesinde saldırganın hareketlerini kısıtlayıcı önlemler almak gerekebilir. Bu noktada da ajanlar avantaj sağlamaktadır. Üç genel strateji vardır; hedefin bağlantısı kesilebilir, saldırganın bağlantısı kesilebilir, hedef ve saldırgan arasındaki bağlantı kesilebilir. Mobil ajanların istenen ağ bileşeninde gezinti yapabilme özellikleri bunların yapılmasını sağlar.

4.1. Dezavantajlar

Mobil ajanlar birçok açıdan IDS sistemlerine fayda sağlamakla birlikte daha fazla fayda beklenmemelidir. Mobil ajanlar bir kaynakta Nüfuz tespit etme yeteneğini geliştirmezler yada yanlış uyarı (false positive) oranını azaltmazlar. Hatta çok iyi tasarlanmadan kullanıldıklarında IDS'in etkinliğini ve başarısını da azaltabilirler. En önemli sorun mobil ajanları Nüfuz tespiti için kullanırken yaşanabilecek güvenlik problemidir. Mobil ajanların bazı zayıflıkları olabilir ve bir saldırgan bu zayıflıkları kullanarak Nüfuz etkisinin yayılmasını ve Nüfuzun tespit edilememesini sağlayabilir.

Mobil ajan uygulamalarında olabilecek güvenlik tehditleri dört genel kategoriye ayrılabilir; agent-to-agent, agent-to-platform, platform-to-agent and other-to-platform. Ajandan ajana olabilecek Nüfuz tehdidi, ajanın kendinde bulunan güvenlik eksikliklerinin ortaya çıkması ve ajanın aynı platformdaki diğer ajanlara Nüfuzlar yapmasıdır. Ajandan platforma olan tehdit ise bir önceki tehdidin ajandan platforma doğru gerçekleşmesidir. Other-to-platform kategorisinde ise dışsal herhangi bir varlık (başka bir ajan grubu veya platformu da olabilir) ajan platformunun güvenliğini tehdit edebilir. Bu tehlikeler, ajanları diğer ajanlardan ve ajan platformlarından izole ederek, kaynaklara kontrollü erişim sağlayarak, yetkilendirilmiş ve korunan iletişim kullanarak önlenbilir.

Klasik hiyerarşik yapıya sahip IDS'lerde güven ilişkisi aşağıya doğru sağlamlık göstermektedir (alt sınıftakiler üst sınıftakilere güvenirken üst seviyedekiler alt seviyedekine güvenmezler yada güven ilişkisi seviyeye göre zayıflar). Hiyerarşinin üst seviyelerindeki bir noktayı ele geçiren saldırgan IDS'in bir kısmını kontrol altında tutabilir hatta merkezi ele geçirirse tüm sistemi kontrol edebilir. Mobil ajanlar tehlikeden kaçabilme özellikleri sayesinde burada bir avantaj sağlarlar.

Mobil ajanların güvenliği için kullanılacak etkin yöntemlerden birisi dijital imzalıdır. Tüm ajanlar sistemde çalışmaya başlamadan önce bir yöneticisi tarafından imzalanmalıdır (sign). Bu yöntem bir saldırganın, ajanın kodunu değiştirmesini veya sahte bir ajanı sisteme sokmasını engeller.

Geleneksel bir IDS ile mobil ajan tabanlı bir IDS'nin güvenlik zayıflık dereceleri neredeyse aynıdır ancak ajanlı sistemlerde yıkım daha büyük olabilir çünkü saldırganın kontrolüne geçen bir platform diğer IDS elemanlarını kolaylıkla etkileyebilir. Saldırgan, gelen ajanları bekletebilir yada sonlandırabilir, yanlış bilgi verebilir yada durum bilgilerini değiştirebilir. Sonucusu en kötü olan etkidir çünkü ajanın davranışlarını değiştirir yada bilgi işleminin etkinliğini azaltır. Bir ajanı bekletmek yada sonlandırmak saldırgan için bazı problemler yaratabilir. IDS, sistemdeki ajanların eksikliğini hissedebilir (kalp atışı mesajlarından) ve bir Nüfuz şüphesi durumuna geçebilir, eksik ajan yerine yenisini yaratabilir, yada diğer ajanları konuyla ilgilenmek üzere görevlendirebilir.

Çok yetenekli bir saldırganın konağı ele geçirmesi ve ajanların durum bilgilerini değiştirmesi durumunda, çoğu sistem ajanın yeteneklerini yetkilerini kısıtlayarak azaltır. Bir ajanın pasaportu gibi nitelenebilecek olan yetki bilgileri vardır. Örneğin, domain authority tarafından verilen

yetki bilgilerini içeren bir dijital sertifika şifrelenerek ve ajanın koduna yerleştirilerek bu özellik sağlanabilir. Bu yetkileri aşmaya çalışan tüm olaylar ajan platformunda gerekli aksiyonun alınmasını sağlayabilir.

Ayrıca ziyaret edilen tüm ortamlarda toplanan bilgiler de değiştirilmemeleri için koruma altına alınabilir. Her platform kendisinde toplanan bilgileri kendi gizli anahtarı ile şifreler, ayrıca bilginin biraz daha sıkı korunması için her ajan kendi açık anahtarıyla da bilgileri şifreler.

5. Mobil ajanlar kullanılarak geliştirilmiş IDS sistemleri

1. Iowa State Üniversitesinde yürütülen bir projede akıllı mobil ajanlar kullanılmıştır. Bu projede mobil ajanlar, bilgi toplayan noktaları dolaşarak bu bilgiler üzerinde veri sınıflandırması (classifier algorithms) yapar, veri temizleyicileri (data cleaners) olarak adlandırılan ajanlar şüpheli durumların ortaya çıkarılmasını sağlar. Sistem hiyerarşik bir yapıya sahiptir, merkezde veri ambarı, yapraklarda (leaves) veri toplayıcıları, arada da classifier ajanları bulunur. Belirli kategorilerdeki Nüfuzlar için özelleşmiş classifier ajanlar vardır ve diğer kategorilerdeki ajanlarla işbirliği yaparak şüpheli durumların ciddiyetini birlikte tespit edebilirler. Bilgilerin analiz edilmesi için analiz ajanlarını bilginin toplandığı yere yollayarak, tüm bilgilerin aggregation noktalarına gönderilmesindeki aşırı yükü ortadan kaldırmaktadır. Ayrıca bu yapı kendisine yapılacak Nüfuzlara karşı da güçlüdür çünkü statik aggregation noktaları yoktur.
2. Event monitoring enabling responses to anomalous live disturbances (EMERALD): SRI international tarafından kötüye kullanım Nüfuzlarının tespiti için geliştirilmiş kural-tabanlı bir sistemdir. Merkezi bir kontrol ve analiz mekanizmasına ihtiyaç duymayan dağıtık bir yapıya sahiptir. Gözleme (monitor), analiz ve yanıt verme bileşenlerinden oluşmaktadır ve büyük ağlarda ve farklı sistemlerde çalışabilir.
3. Autonomous agents for intrusion detection (AAFID): Ağdaki bilgisayarları ajanlar ile kontrol eden bir IDS'dir. AAFID ekibi çoğu IDS'de bulunan, tek noktada gerçekleşen sorunun tüm sistemi etkilemesi problemini, ağdaki tüm bilgisayarlara aynı yetenekteki ajanları yayarak aşmaktadır. Her bilgisayarda sabit olarak tranceiver olarak adlandırılan bir bileşen vardır. Bilgisayar üzerindeki tüm ajanlar aynı bilgisayardaki tranceivera rapor gönderirler. Bir veya birden fazla "monitor" tranceiverlardan sonuçları alır. Yani monitorlar ağ genelindeki dataya erişirler. Böylece birden fazla bilgisayarı kapsayan Nüfuzlar da tespit edilebilir.
4. NIST'te mobil ajanlar ile Nüfuzlara dayanıklı bir sistem geliştirilmiştir. Saldırganın, ağı incelediğinde ajanları tespit edememesi sağlanmıştır. Buna ek olarak, Nüfuzya uğrayan bir bilgisayardaki ajan, normal çalışmasına devam eden başka bir bilgisayara kendini aktarabilmektedir.
5. Intrusion detection and tracking system (IDTS)

6. Sonuç / Conclusion

Mobil ajanların Nüfuz tespit sistemlerindeki başarısını, ölçeklenebilirlik ve dayanıklılık konularında sağlayabileceği faydaları inceledik. Mükemmel bir çözüm olmamakla birlikte, mobil ajan teknolojisi IDS'lerden beklenen ideal davranışların gerçekleşmesi için büyük katkılar sağlama imkanına sahiptir. Sadece Nüfuz tespit yöntemleri ajanlardan faydalanmakla kalmayıp, önemli bir gereklilik olan Nüfuzlara karşılık verme yöntemleri de çok büyük gelişmeler gösterebilir. Mevcut IDS'lerde mobil ajanlar çok fazla kullanılmadığı için teknolojinin bu alana

dođru hızlı bir geiř yapmasını beklemek dođru olmaz. Fakat adım adım teknoloji IDS'lere yerleřmektedir.

Kaynaka / References

- [1] Wayne A. Jansen, 2002. Intrusion detection with mobile agents, *Computer Communications*, 25 (2002) 1392-1401
- [2] E. Biermann, E. Cloete, L.M. Venter, 2001. A comparison of intrusion detection systems, *Computers&Security*, 20 (2001) 676-683
- [3] Peter Mell, Donald Marks, Mark McLarnon, 2000. A denial-of-service resistant intrusion detection architecture, *Computer Networks* 34 (2000) 641-658
- [4] V. Paxson, 1999. Bro: a system for detecting network intruders in real time, *Computer Networks* 31 (1999) 2435-2463
- [5] Dr Rhodri M. Davies, *Firewalls, intrusion detection systems and vulnerability assessment: a superior conjunction*, Vistorm Ltd.
- [6] G. Pietro Picco, 2001. Mobile agents: an introduction, *Microprocessors and microsystems*, 25 (2001) 65-74
- [7] M.K. Perdikeas, 1999. Mobile agent standards and available platforms, *Computer networks*, 31 (1999) 1999-2016
- [8] Midori Asaka, 1999. Information gathering with mobile agents for an intrusion detection system, *Systems and computers in Japan*, Vol. 30, No.2, 1999