

Saldırı Tespit Sistemlerinde Ajan Sistemlerin Kullanımı

Using Agent System In Intrusion Detection System

Esra SÖĞÜT

Bilgisayar Mühendisliği Bölümü,
Gazi Üniversitesi Teknoloji Fakültesi
Ankara, Türkiye
esrasogut@gazi.edu.tr

O. Ayhan ERDEM

Bilgisayar Mühendisliği Bölümü,
Gazi Üniversitesi Teknoloji Fakültesi
Ankara, Türkiye
ayerdem@gazi.edu.tr

Aydın ÇETİN

Bilgisayar Mühendisliği Bölümü,
Gazi Üniversitesi Teknoloji Fakültesi
Ankara, Türkiye
acetin@gazi.edu.tr

Özet

Saldırı tespit sistemlerinde, ana sistemin yanı sıra ağı ve ağ bileşenlerinin performansları üzerinde daha iyi bir gelişme sağlanması amaçlanmaktadır. Saldırıların veya tehditlerin sistem içerisinde yayılmadan önce giriş noktalarında engellenmesi ve durdurulması gerekmektedir. Mobil ajan teknolojisi bu amaçları gerçekleştirmek için kullanılmaktadır. Bir sistemden diğerine bağımsız şekilde hareket edebilen ve hedef sistem üzerinde işlevini sürdüren yazılım veya cihazlar mobil ajanlar olarak adlandırılmaktadır. Merkezi olmayan dağıtık ortamdaki saldırıların tespiti için geliştirilmiştir. Bu çalışmada, mobil ajan temelli saldırı tespit sistemleri incelenmektedir. Saldırı tespit sistemlerinde mobil ajanlar vasıtasıyla gerçekleşen performans değişiklikleri ve geliştirilen teknikler örnek uygulamalara yer verilerek gösterilmektedir.

Anahtar Kelimeler

Mobil Ajanlar, Saldırı Tespit Sistemleri, AAFID, IDA

I. GİRİŞ

Saldırı tespit sistemleri (STS), ağ kaynaklarının ya da bilgisayar sistemlerinin hedef alındığı saldırılar ile ilgilenmektedir. Bilgisayar sistemlerine yapılan saldırıların tespit edilmesi ve saldırılara ait özelliklerin belirlenmesi STS çalışma alanlarıdır. Saldırı kaynağının belirlenmesi ve daha önce tanımlanan çerçeveye sahip olan saldırıların fark edilip tekrar uygulanması durumunda tespit edilmesi STS'ler için önemli konulardır [1]. Saldırı tespiti için farklı alanlarda yapılan çalışmalardan biri de dağıtık mimari yapısıdır. Dağıtık mimarinin dağıtık saldırıların daha hassas tespit edilmesinde kullanılması için çalışmalar yapılmaktadır. İstemci-sunucu ve merkezi yaklaşımların sınırlamalarını aşmak için dağıtık mimari ile mobil ajan sistemleri kullanılmaktadır. Ajan tabanlı sistemlerde merkezi bir istasyon bulunmadığı için merkezi bir başarısızlık noktası da bulunmamaktadır. Ayrıca ajanlar otonom hareket edebildiği için aralarında hiyerarşik bir dizilim de yoktur. Ajanlar diğer ajanlardan bağımsız olarak hareket edebilir ve farklı görevleri yerine getirebilirler.

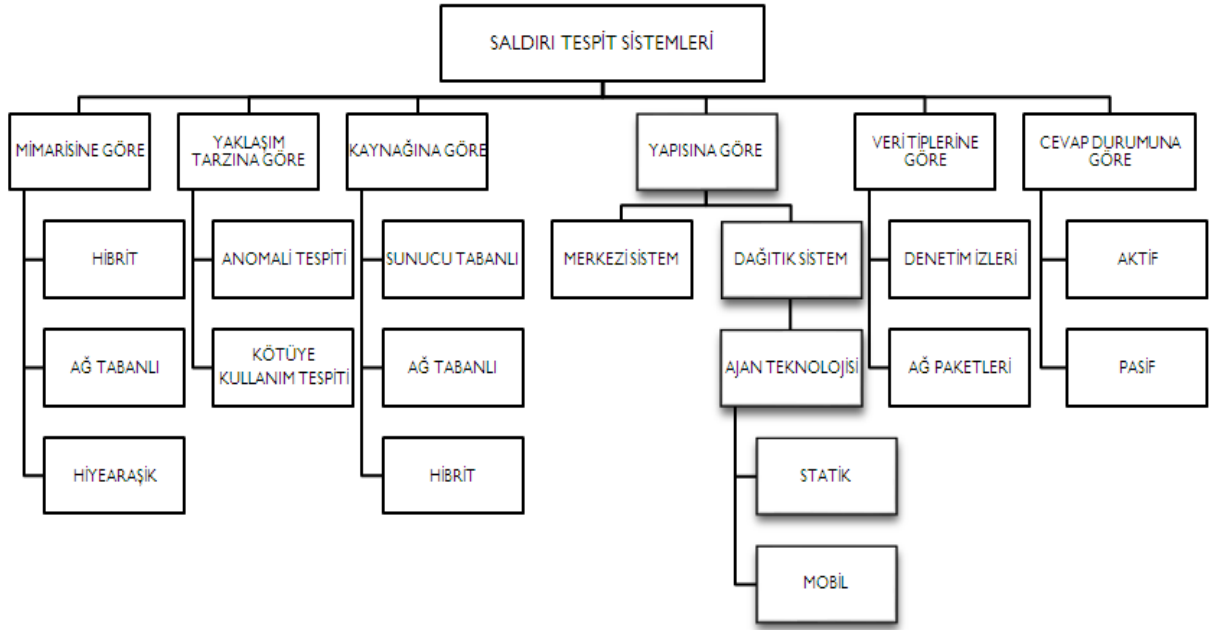
STS'lerde mobil ajan kullanımıyla ilgili yapılmış birçok çalışma vardır. Barrus ve ark. 1998 yılında yaptıkları çalışmada saldırıları durdurmak için işlemlerin otomatik olarak yapılması gerektiğini belirtmişlerdir. Bunu sağlamak için heterojen bir ağda gerçek zamanlı algılama yapan ve yanıt veren otonom ajanların kullanılmasını önermişlerdir [2]. Jai Sundar ve ark. 1998'de dağıtık mimari kullanarak Autonomous Agent For Intrusion Detection sistemini geliştirmiştir [3]. Zhang ve ark. 2000'de ve Thomas Toth ve ark. 2002'de dağıtık mimari kullanarak mobil ajan teknolojisi çalışmalarını sürdürmüştür [4,5]. 2015'de Al-Yaseen ve ark. yaptıkları çalışmada çoklu ajan ortamlarında STS için makine öğrenmesi yöntemlerini kullanmışlardır. Yaptıkları çalışmada C4.5 ile K-Means algoritmalarını kullanarak ajan sistemler için melez bir uygulama önermişlerdir [6].

Bu çalışmada, Mobil Ajan Teknolojisi incelenerek, bu teknolojinin saldırı tespit sistemlerinde kullanılabilirliği hakkında bilgi verilmiştir. Mobil ajanların sahip olduğu olumlu ve olumsuz davranışlar hakkında değerlendirme yapılmıştır. Ayrıca, saldırı tespit sistemlerinde kullanılan farklı mobil ajan uygulamaları birlikte ele alınarak kıyaslamaları yapılmış ve sonuçları tablo halinde sunulmuştur.

II. SALDIRI TESPİT SİSTEMLERİ

Saldırı varlığını tespit etmek için antivirüs, güvenlik duvarı ve STS gibi çeşitli araçlar/yazılımlar araştırma kuruluşlarında olduğu kadar günlük hayatta da kullanılmaktadır. Bu araçlar/yazılımlar algılama yetenekleri bakımından incelendiğinde STS'nin diğerlerine göre daha güçlü olduğu görülmektedir [7]. STS'ler, ağ veya sistem üzerindeki kötü niyetli faaliyetleri veya kural ihlallerini izleyen cihaz veya yazılım uygulamalarıdır. STS'ler ile elde edilen sonuçlar sistem veya ağ yöneticisine rapor edilir ve gerekli işlemlerin yapılması için uyarılarda bulunulur [8].

STS'leri sınıflandırmak için çeşitli yaklaşımlar bulunmaktadır. Bu yaklaşımlar Şekil 1'de gösterilmektedir.



Şekil 1 STS sınıflandırılması [9]

Şekil 1'de görüldüğü üzere STS sınıflandırması 6 farklı yaklaşıma göre yapılmış ve Ajan Teknolojisinin kullanıldığı yaklaşım belirtilmiştir. Buna göre STS, yapısına göre incelendiğinde dağıtık sistemler Ajan Teknolojisini içermektedir. Ajan Teknolojisi de statik ve mobil olmak üzere iki bölüme ayrılmaktadır. Bu çalışmada, sabit bir sistem üzerinde işlevlerini sürdürmesinden dolayı statik ajan teknolojisi kapsam dışı tutulmuştur.

III. MOBİL AJAN SİSTEMLERİ

Dağıtık sistemlerin geliştirilmesi ile saldırı tespiti yapmak için yazılım ajanları kullanılmaya başlanmıştır. Bunun sonucunda mobil ajan teknolojisi bu alanda kendini göstermeye başlamıştır. Mobil ajanlar, kendi kendine yeten ve tanımlanabilir otonom bilgisayar programlarıdır. Bunlar sahip oldukları kodları, verileri ve çalışma durumları ile birlikte heterojen ağ yapılarına sahip bilgisayar sistemlerinde hareket edebilmektedir [10]. Bu tür ajanlar, saldırı tespit sistemleri dışında uzay aracının otomasyonu, oyun oynama, direksiyon kullanımı, tıbbi teşhis, robotik, dilin anlaşılması ve problem çözümü gibi çeşitli endüstriyel uygulamalarda da kullanılmaktadır [11].

Mobil ajanların kullanımı ile dağıtık yapıda veri toplama ve veri işlemenin birden fazla düğümde yapılması sağlanmaktadır. Düğüm sayısının fazla olmasına rağmen, yapılan incelemelere göre işlem yanıt süresinde ve ajan boyutunda iyileşme yapılabileceği tespit edilmiştir [7].

Mobil ajanlar, program kodlarının farklı ortamlarda çalıştırılması özelliğinden faydalanmaktadır. Ajanlar, bir makinedeki çalışmasına ara vererek veya çalışmasını sonlandırarak başka bir makineye geçebilir ve çalışmalarına kesintisiz devam edebilirler.

STS'lerde Mobil ajanların kullanımı birçok avantaj sağlamaktadır. Bunun yanı sıra Mobil ajan kullanımının dezavantajları da bulunmaktadır.

A. Avantajlar

Mobil ajanların kullanılabilmesi için ağdaki her makinenin ajan platformuna sahip olması gerekmektedir. STS'lerde statik bileşenler kullanmak yerine mobil ajan tabanlı sistemlerin kullanılması birçok avantaj sunmaktadır. STS'lerde mobil ajan kullanımının avantajları aşağıda belirtilmektedir [12,13].

- Ağ yükünü azaltma: Büyük miktarda veriyi veri işleme birimine göndermek yerine, işleme algoritmasını (ajanı) verilere taşımak daha basit olabilir.
- Ağ gecikmesini azaltma: Mobil ajanlar, çevredeki değişikliklere gerçek zamanlı olarak yanıt verdikleri için ağın başka bir yerinde olan merkezi koordinatörle iletişim kurmaya gerek kalmadan hızlı yanıt verebilir.
- Ölçeklenebilirlik: Ağdaki işlem öğelerinin sayısı arttıkça, ajanlar çoğalabilir ve ağdaki yeni makinelere gönderilebilir.
- Hata toleransını artırma: Mobil ajanlar çevrelerindeki değişikliklere dinamik ve otonom olarak tepki verdikleri için hataya karşı dayanıklı ve sağlam yapıya hale gelirler.
- Eş zamanlı ve otonom yürütme: Mobil ajanlar, ana makine müdahalesi olmadan otonom ve eş zamansız olarak çalışabilir. Ana makineye tekrar bağlanabilir.
- Platform bağımsızlığı: Ajanlar, ana makine platformundan bağımsız olarak çalışabilir.
- Dinamik ve statik uyarılma: Ajanların dinamik davranışı nedeniyle sistem çalışma zamanı yeniden yapılandırılabilir. Statik uyarılma özelliği ile tüm sistem yeniden başlatılmaksızın ajanların algoritmaları güncellenebilir.

B. Dezavantajlar

Ajan tabanlı STS'lerin sahip olduğu avantajların yanı sıra, güvenlik, kod boyutu ve performans gibi konularda bazı problemleri bulunmaktadır [12,14].

- Güvenlik: Kötü amaçlı bir mobil ajan, ana makineye veya başka bir mobil ajana zarar verebilir, işleyişe engel olabilir ve sistemi aksatabilir.
- Kod boyutu: Ajanın gerekli kodu ağ üzerinden aktarması zaman kaybına sebep olabilir fakat her bir ana makine ajanının bu kodu yerel olarak bir kez depolaması yeterlidir.
- Performans: Ajanlar genellikle farklı platformlar arasında kolaylıkla taşınabilmek için komut dosyası veya yorumlanmış dillerde yazılmıştır. Bu durum ajanların hareketini yavaşlatmaktadır.

- Öncelikli bilgi eksikliği: Bir sistemin nasıl yapılandırıldığı, verilerin nasıl düzenlendiği ve sistem yükünün nasıl ayarlandığı konularında mobil ajanların önceden bilgi sahibi olması önemlidir.

IV. ÖRNEK AJAN TABANLI STS UYGULAMALARI

Bilgisayar ağlarında mobil ajanların kullanımı ile saldırı tespit sistemlerine yeni bakış açısı kazandırılmıştır. Literatürde çok sayıda mobil ajan tabanlı STS bulunmaktadır. Bu örnek uygulamalara karşılaştırmalı olarak Tablo 1'de yer verilmektedir.

Tablo 1. Örnek Ajan tabanlı STS uygulamalarının karşılaştırılması

Model	Yaklaşım	Avantajlar	Dezavantajlar	Kaynak No
Autonomous Agents For Intrusion Detection (AAFID)	Ana bilgisayar tabanlı mobil ajan yaklaşımı	Ölçeklenebilir sistem yapısı Toplanmış ve önışleme tabi tutulmuş bilgi kullanımı	Ajanlar ve monitör arasındaki katmanın saldırı tespitinde gecikmeye sebep olması Monitörlerin tek başarısızlık noktası olması	3
Intrusion Detection Agent System (IDA)	Mobil ajan yaklaşımı	Saldırgana ait izlerin takibi Basit sistem yapısı	Sınırlı derecede ölçeklenebilirlik. Merkezi veri toplama	15
Intelligent Mobile Agents for Intrusion Detection System (IMA-IDS)	Ana bilgisayar tabanlı mobil ajan yaklaşımı	Toplayıcı ajanların sonuçları yöneticiye bildirmesi Anormallik tespitinde alarm üretilmesi	Merkezi veri toplama	15
Micael	Mobil ajan yaklaşımı	Ajanların bilgi toplama dışında da kullanılması Ajanların olaylara tepki vermesi Taşınabilir sistem yapısı	Yalnızca JAVA'yı destekleyen platformlarda çalışması	15
Intelligent Agents for Distributed Intrusion Detection System (IA-DIDS)	Ana bilgisayar tabanlı mobil ajan yaklaşımı	Ağdaki ana makineler üzerinde otonom çalışma	-	15
Preemptive DIDS	Ağ tabanlı mobil ajan yaklaşımı	Saldırı tespit edildiğinde, saldırının engellenmesi için şüpheli paketlerin işleme alınmadan sistem dışına atılması	-	15
Distributed Soft Computing for Intrusion Detection System (DSCIDS)	Hibrit yaklaşım	Hiyerarşik sistem yapısı Katmanlar arasında rahat iletişim Farklı hesaplama algoritmaları	Ajanların dağılımının yeterli ve düzenli olmaması Hesaplama algoritmalarının tespit konusunda çalışmasının tartışmaya açık olması	16
Multi-Level and Secured Agent-based Intrusion Detection System (MSAIDS)	Kötüye kullanım tespiti	Mobil ajanların güvenliğine ek olarak kaydedilmiş durum mekanizmasının kullanımı Ajanların iyi organize edilmesi	Her seviyede saldırı tespiti için aynı algoritma kullanılması ile raporlamada gecikme yaşanması Değişik saldırı davranışlarına göre yeterli tedbirler bulunmaması	17
Mobile Agent for Network Intrusion Resistance	Hibrit yaklaşım	Geleneksel dağıtık tespit sistemlerinin hiyerarşik yapısından farklı olması	Saldırı tespitinin önemli bölümünün yapıldığı yerde tek bir kontrol merkezi olması Bu merkezin ele geçirilmesi ile sisteme ciddi zararların verilebilmesi	18

Örnek ajan tabanlı STS uygulamaları yaklaşım biçimi, sahip olunan avantaj ve dezavantaj kriterlerine göre değerlendirilmektedir. Yaklaşım biçimi olarak ana bilgisayar tabanlı mobil ajan dışında hibrit ve kötüye kullanım tespiti yaklaşımları da kullanılmaktadır. Her örnek uygulamanın kendine özel avantajları ve dezavantajları bulunmaktadır. Ölçeklenebilir, basit, taşınabilir veya hiyerarşik sistem yapılarına sahip olunması avantajlar arasında yer almaktadır. Merkezi şekilde veri toplama gerçekleştirilmesi, tek bir kontrol merkezinin bulunması veya gecikmelerin yaşanması dezavantajlar arasında kendini göstermektedir.

V. SONUÇ

Bu çalışmada, ajan tabanlı sistemlerin STS'lerde kullanımı incelenmiştir. Ajan tabanlı STS örnek uygulamaları değerlendirilmiş ve karşılaştırmaları yapılmıştır.

Saldırı tespit sistemlerinde ajan tabanlı sistemlerin kullanımı ile ilgili birçok çalışma bulunmaktadır. Farklı yapılarda ve özelliklerde olan çalışmalar ile elde edilen sonuçlar incelenmiştir. Buna göre bir takım çıkarımlar yapılmıştır. Bunlar:

- STS'nin tamamında ajanların kullanılması tam anlamıyla işlevsellik sağlamayabilir.
- Bazı bileşenlerin statik olması sistem çalışması için verimli olabilir.
- Sistemlerin tümünde mobil anlayışın yer alması sisteme fazladan yük gelmesine sebep olabilir.
- Taşınabilirlik sistemde gerekli görülen bölümlerde ve zamanda yapılmalıdır.
- Ajanların kötü amaçlı kullanılabilmesi sistem güvenliğini tehlikeye atabilir. Yeni güvenlik çözümlerinin geliştirilmesi gerekmektedir.
- Yapılarından ve kullanım şekillerinden dolayı farklı boyutlarda olan kodların ajan tarafından aktarılması gecikmeli olabilir. Bunun önüne geçilebilmesi için farklı sistem şekilleri veya yöntemleri kullanılabilir.
- Sistem yapılandırılması ve işleyişi konularında ajanların bilgi sahibi olması gereklidir. Bunu sağlamak için ajan eğitimi, ajan keşfi ve ajan kullanımı konularında yeni çözümlerin geliştirilmesi gerekmektedir.
- Yakın gelecekte çok daha fazla bilgi toplayıcı ajanın kullanılacağı ve toplanan bilgilerin analiz edilmesi için daha fazla ajana ihtiyaç olacağı öngörülmektedir.
- Gelecekte özelleşmiş ajanların kullanılması ile analiz ajanlarının birden fazla tip saldırıyı tespit edebilecek duruma geleceği öngörülmektedir.
- Her sistemde birden fazla ajanın birlikte çalışabileceği öngörülmektedir.

Farklı sistemlere farklı ajan tabanlı öneriler sunulabilmektedir. Gelecekte yapılacak çalışmalar için daha gelişmiş, dezavantajları azaltılmış ve performans düzeyi iyileştirilmiş ajan sistemlerinin kullanılacağı öngörülmektedir.

KAYNAKLAR

[1] Söğüt, E. Gelişmiş Isırcı Tehdit Tespit Yöntemleri Ve Bir Uygulaması, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, 2016.

[2] Barrus, J. (1998). A Distributed Autonomous-Agent Network-Intrusion Detection and Response System. Proceedings of the 1998 Command and Control Research and Technology Symposium. June-July. Monterey, CA.

[3] Balasubramanian, J.S., Garcia-Fernandez, J. O., Isacoff, D., Spafford, E., Zamboni, D., An Infrastructure for Intrusion Detection using Autonomous Agents, COAST Technical Report 98/05, June 11, 1998.

[4] Spafford, E. H., Intrusion Detection Using Autonomous Agent, Computer Networks, 2000, 3(4): 547-570.

[5] Krügel, Christopher, Thomas Toth. Flexible, mobile agent based intrusion detection for dynamic networks, European Wireless. 2002.

[6] Al-Yaseen, W. L., Othman, Z. A., Nazri, M. Z., Hybrid Modified k-Means with C4.5 for Intrusion Detection Systems in Multi-agent Systems, The Scientific World Journal, Volume 2015, Article ID 294761, 14.

[7] Shah, B., Trivedi, B., Improving Performance of Mobile Agent Based Intrusion Detection System, IEEE International Conference on Advanced Computing & Communication Technologies-2015.

[8] Internet: <http://suricata-ids.org/> [Son erişim tarihi: 05.05.2017].

[9] Onashoga, S.A., Adebayo D. Akinde A., Strategic Review of Existing Mobile Agent- Based Intrusion Detection Systems, Issues in Informing Science and Information Technology Volume 6, 2009.

[10] Christopher, K., Thomas, T., Applying Mobile Agent Technology to Intrusion Detection, In ICSE Workshop on Software Engineering and Mobility, 2001.

[11] Trivedi, B. H., Mobile Intelligent Agents in Intrusion Detection, proceeding of NCC-06 National Conference on Computing and Communication, Hyderabad, 13th-15th July- 2006.

[12] Jain P., Raghuwanshi, S., Pateria, R., New Mobile Agent-Based Intrusion Detection Systems for Distributed Networks, International Journal of Wireless Communication Volume 1, Issue 1, 2011, pp-01-04.

[13] Albag, Hakan. Network & Agent Based Intrusion Detection Systems, TU Munich Dep. of Computer Science, Istanbul Technical University, 2001.

[14] Srivastava, S., Gupta N., Saugata, G., Chaturvedi, S., A Survey on Mobile Agent based Intrusion Detection System, International Symposium on Devices MEMS, Intelligent Systems & Communication (ISDMISC) 2011.

[15] Khobragade, S., Padiya, P., Distributed Intrusion Detection System Using Mobile Agent, International Journal of Engineering and Innovative Technology (IJEIT), Volume 5, Issue 4, October 2015.

[16] Abraham, A., Jain, R., Thomas, J., Han, S. Y., D-SCIDS: Distributed soft computing intrusion detection system. Journal of Network and Computer Application, 30, 81-98, 2007.

[17] Sodiya, A. S., Multi-level and secured agent-based intrusion detection system. Journal of Computing and Information Technology, 14(3), 217-223, 2006.

[18] Wang, H. Q., Wang, Z. Q., Zhao Q., Wang G. F., Zheng R. J., & Liu, D. X., Mobile agents for network intrusion resistance. APWeb Workshops 2006, LNCS 3842, pp 967-970, 2006.