

## Güvenlik Uygulamaları için Ajan Sistemler ve Otonomi

Özlem Ünlü<sup>1\*</sup>, Aydın Çetin<sup>2+</sup>

<sup>1</sup>TÜBİTAK ULAKBİM, Ankara, Türkiye

<sup>2</sup>Teknoloji Fakültesi Bilgisayar Mühendisliği Bölümü, Gazi Üniversitesi, Ankara, Türkiye

\*Corresponding author: ozlemkilic\_aks@yahoo.com

+Speaker: ozlemkilic\_aks@yahoo.com

Presentation/Paper Type: Oral/ Full Paper

**Özet** – Gelişen bilgisayar ve iletişim teknolojileri sonucunda güvenlik önemli bir konu haline gelmiştir. Güvenlik açıkları yetkilendirme, veri bütünlüğü sağlama, ağ güvenliği gibi sistemin çalışmasında etkili kısım veya kısımlarda olabilmektedir. Bir sistemin güvenliği bir takım araç-politikalarla sağlanır. Veri bütünlüğü için çeşitli yedekleme-birleştirme politikaları kullanılırken, sistemde var olan zararlıların tespiti için tarama araçları kullanılmaktadır. Güvenlik uygulamalarında araçların kullanımında etkin bir yönetim ve karar destek yapısı oluşturmak için ajan sistemlerden etkin bir şekilde yararlanmak mümkündür. Bu çalışmada Güvenlik Uygulamaları için ajan kavramı ve ajanlarda otonomi çalışmaları incelenmiştir.

**Anahtar Kelimeler** – Güvenlik, otonom, ajan, ajan tabanlı mimari

### I. GİRİŞ

Bilgisayar önceleri uzun süreli hesaplamalı işlemleri gerçekleştirmek için üretilse de günümüzde farklı formlarda hayatımızın her alanında kullanılmaktadır. Önceleri sadece hesaplama için kullanılırken kullanıcı ara yüzü geliştirilmesi ile birlikte 7' den 70' e herkesin kullandığı bir araç haline gelmiştir. İnternetin gelişmesi ile birlikte lokal çalışabilme kısıtından kurtulmuş, bu sayede bireysel bankacılık işlemleri, elektronik aletler gibi farklı alanlarda da kendine yer bulmuştur. Fabrikalar, Savunma Sanayii, elektronik aletler, kara, hava ve deniz taşıtları, akıllı ev sistemleri vs. gibi çok geniş bir yelpazede kullanılmaktadır. Bu kadar çok alanda kullanılıyor olması ve gerçekleştirdiği işlemlerin önemli olması bilgisayar sistemlerinin güvenli olması gerekliliğini de beraberinde getirmektedir.

Bu güvenlik açıkları yetkilendirme, veri bütünlüğü sağlama, ağ güvenliği gibi sistemin çalışmasında etkili kısım veya kısımlarda olabilmektedir. Bir sistemin güvenliği bir takım araç-politikalarla sağlanır. Örneğin veri bütünlüğü için çeşitli yedekleme-birleştirme politikaları kullanılırken, sistemde var olan zararlıların tespiti için tarama araçları kullanılmaktadır. Bu çalışmada Güvenlik Uygulamaları için ajan kavramı ve otonomi konularında yapılan çalışmalar incelenmiştir.

### II. OTONOMİ VE AJAN KAVRAMI

Otonom bir sistemin kendi kendine karar verebilmesidir. Otonom bir sistem dediğimizde aklımıza robotlardan, akıllı ev gereçlerine, savunma sistemlerinden, güvenlik sistemlerine kadar birçok alanda çalışan sistemlerin kendi kendine karar verebilme yetenekleri gelmektedir.

Otonom bir sistem, üst düzey amaç ve yönü anlayabilir. Böyle bir sistem, bu anlayıştan ve çevresi algısından, istenen bir durumu ortaya çıkarmak için gerekli önlemleri alabilir.

İnsan gözetim ve denetimine bağlı olmaksızın, bir takım alternatiflerden bir dizi eylem karar verebilme yeteneğine sahiptir[1].

Otonom sistemler sadece robotlar ve insansız araçlarla sınırlanmaz. Bunun dışında bir fonksiyonun otonom olmasından söz edilebildiği gibi bir koruma sistemi yazılımı için de otonomluktan bahsedilebilir.

Otonominin seviyelendirmeleri çeşitli gruplar tarafından farklı farklı yapılmıştır. US Navy Office of Naval Research and the UK's Systems Engineering for Autonomous Systems Defence Technology Centre tarafından yapılan seviyelendirme 6 seviyeden oluşur ve aşağıdaki gibidir [2]:

*Seviye 1, İnsan Kullanımında olan:* Sistemdeki tüm faaliyet, insan tarafından başlatılan çevrenin doğrudan bir sonucudur, ancak algılanan verilere yalnızca bilgi yanıtları olabilir.

*Seviye 2, İnsan Desteğinde olan:* Sistem, insanın girişiyle paralel bir faaliyette bulunabilir, insanın istenen aktiviteyi gerçekleştirme kabiliyetini artırır ancak insanın girdisi olmaksızın hareket etme kabiliyeti yoktur. Buna otomobil otomatik transmisyon ve kaymaz frenler örnektir.

*Seviye 3, İnsan Tarafından Yetkilendirilen:* Sistem, delege bazında sınırlı kontrol etkinliği gerçekleştirebilir. Seviye, bir insan girdisi tarafından aktive edilmek veya devre dışı bırakılması gereken otomatik uçuş kontrolleri, motor kontrolleri ve diğer düşük seviye otomasyonu kapsar ve insan işlemi ile karşılıklı dışlama içinde hareket eder.

*Seviye 4, İnsan Denetimli:* Sistem, bir insan tarafından üst düzey izinler veya yön verilen çok çeşitli aktiviteleri gerçekleştirebilir. Sistem iç operasyonları ve davranışları

hakkında yeterli bilgi verir ve insan tarafından kolaylıkla anlaşılabilir ve uygun şekilde yeniden yönlendirilir. Sistem, mevcut yönlendirilmiş görevlerin kapsamı dışındaki davranışları kendiliğinden başlatma kabiliyetine sahip değildir.

*Seviye 5, Karışık Başlatan:* Hem insan hem de sistem, algılanan verilere dayalı davranışları başlatabilir. Sistem, davranışını açıkça ve dolaylı olarak koordine edebilir. İnsan, sistemin davranışlarını, kendi davranışlarını anladığı şekilde anlayabilir. Sistemin insan operatörlerine göre yetkisini düzenlemek için çeşitli araçlar sağlanmaktadır.

*Seviye 6, Tam Otonom:* Sistem, planlanan tüm faaliyet koşullarını çevre koşullarının tümü boyunca yerine getirmek için herhangi bir müdahaleye gerek duymaz.

Sistemin otonomi seviyesine çalışma prensibi, gereksinimleri, özellikleri, yapılacak iş, kaynak kısıtı, güvenlik vb. sebeplere göre karar verilir. Ve sistem bu otonomi seviyesinde kullanıma sunulur.

Ajan belli bir iş için üretilmiş, otonom yazılım veya donanımlardır. Ajanlar bir sefer başlatıldıktan sonra belirlenen hedefi gerçekleştirmek için çalışırlar ve sonlandırılıncaya kadar çalışmaya devam ederler.

Otonomi kavramı gibi ajan kavramı da farklı gruplar tarafından tanımlanmıştır. MuBot ajan kavramını “Ajan terimi, iki ortogonal kavramı temsil etmek için kullanılır. İlki ajanın özerk yürütme kabiliyetidir. İkincisi, temsilcinin alan odaklı mantık yürütme yeteneğidir.” [4] şeklinde tanımlanmıştır. Artificial Intelligence: a Modern Approach (AIMA) ajan kavramını “Bir ajan, çevresini algılayıcılarla algılayan ve o ortamda efektörler vasıtasıyla hareket eden olarak görülebilir.” şeklinde tanımlanmıştır[5]. Pattie Maes’ in tanımı “Otonom ajanlar, karmaşık dinamik bir çevrede yaşayan, bu ortamda kendiliğinden hareket eden, hissetmek ve hareket etmek için tasarlanmış hesaplama sistemleridir ve böylece tasarlanmış oldukları bir dizi amaç veya görev gerçekleştirirler.” şeklindedir [6]. IBM “Akıllı ajanlar, bir dereceye kadar bağımsızlık veya özerklik ile bir kullanıcı veya başka bir program adına bazı işlemler gerçekleştiren yazılımlardır ve bunu yaparken, kullanıcının hedef veya arzularına ilişkin bazı bilgi veya gösterimleri kullanır.” tanımını yapmıştır [7].

Bazı gruplar ajan tanımında ajanların özelliklerini belirtmişlerdir. The Wooldridge-Jennings’ ajanları karakteristik özellikler içeren bir donanım veya (genellikle) yazılım tabanlı bilgisayar sistemi olarak tanımlamakta ve ajanların karakteristik özelliklerini otonomi, sosyal kabiliyet, tepkisellik ve etkinlik yanlısı olarak sınıflandırmaktadır. Bu karakteristik özellikler:

- *otonomi:* Ajanlar, insanların doğrudan müdahale etmeksizin çalışırlar ve eylemleri ve iç halleri üzerinde bir takım kontrolleri vardır,

- *sosyal kabiliyet:* ajanlar, diğer araçlar (ve muhtemelen insanlar) ile bir tür ajan-iletişim dili ile anlaşılırlar,

- *tepkisellik:* ajanlar çevreyi algılayıcılar (fiziksel dünya, bir kullanıcı, grafiksel bir kullanıcı ara yüzü, diğer ajanlardan oluşan bir koleksiyon, internet veya belki de bunların hepsi bir arada olabilir) ve içinde meydana gelen değişikliklere zamanında tepki verir,

- *etkinlik yanlısı:* ajanlar yalnızca çevreye tepki olarak davranmazlar, inisiyatif alarak hedefe yönelik davranış sergilerler,” şeklinde ifade edilmektedir [8].

Tolk ve Uhrmacher ise akıllı yazılım ajanlarının temel karakteristik özelliklerini yerleşiklik, otonomi ve esneklik olarak tanımlar. Diğer bir ifadeyle “Ajan yerleşiktir, çevresini algılar ve çevrede hareket eder, Ajan otonomdur, insanın veya başkalarının doğrudan müdahalesi olmadan çalışabilir ve Ajan esnektir, bu da hedeflerini gerçekleştirmek için tepkisel davranış ve çekingenlik arasında arabuluculuk yapabileceği anlamına gelir,” [8].

Ajan yazılımlar ağda, veri tabanında vs. görev yaparlar. III. Bölümde güvenlik uygulamaları için geliştirilen ajan tabanlı mimariler incelenmektedir.

### III. GÜVENLİK UYGULAMALARI İÇİN AJAN KAVRAMI VE OTONOMİ

Güvenlik kişi, kurum yada kuruluşların içeriden veya dışarıdan gelebilecek tehdit, taciz, sabotaj, yangın gibi olaylara karşı alınacak tedbirler zincirine denir [9]. Bilgi teknolojileri perspektifinden ise kişi veya kurumların sahip olduğu donanım, yazılım, sistem veya bilginin içeriden veya dışarıdan gelebilecek saldırılara karşı alınabilecek tedbirler, gerçekleştirilmiş saldırıların etkilerini azaltacak veya giderebilecek mekanizmalar bütünü olarak tanımlanabilir.

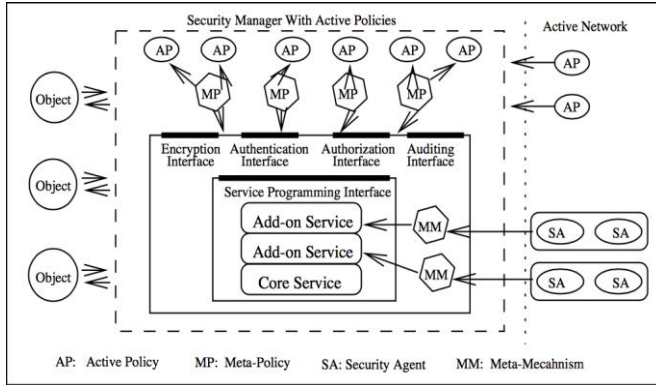
Bilgi güvenliği kullandığımız donanım güvenliği, ağ güvenliği, veri bütünlüğü, yetkilendirme gibi konuları kapsamaktadır. Bilgi güvenliğini sağlamak için sistem ve ağ yöneticileri çeşitli tedbirler geliştirmekte, mevcut saldırıları anlayıp hasarlarını gidermek için taramalar yapmaktadır. Tarama yerel-tabanlı veya ağ-tabanlı yapılabilmektedir. Son yıllarda literatürde ajan tabanlı tarama (güvenlik ajanları) üzerine araştırmalar yapılmaktadır. Sızmalar için Sızma Tespit (IDS) ve Sızma Önleme (IPS) Sistemleri donanım(router) veya sunucu üzerinde kullanılabilir.

Dağıtık güvenlik mimarisi olan Ajan Tabanlı Güvenlik Mimarisi;

- Çeşitli politikaları ve mekanizmaları destekleyebilecek kapasitedir,
- Politikaları ve mekanizmaları ekleyebilir, değiştirebilir veya iptal edebilir,
- Uygulamaların, sistemden istedikleri güvenlik garantilerinin türünü belirtmesini sağlar,

- Bu özelleştirilmiş politikaları ve mekanizmaları dinamik olarak zorlar,
- Politikayı, politikayı bilmeleri gereken uygulamalar ve sistemler için kısıtlar[12].

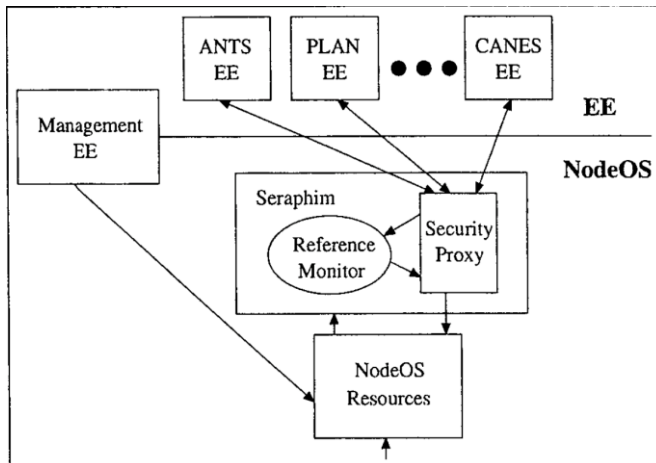
Ajan tabanlı bir güvenlik mimarisi olan Cherubim mimarisinin amacı, özellikle erişim kontrol şemalarında uygulanabilir ve genişleyebilen uygulama önlemlerini destekleyen ajan tabanlı bir güvenlik çerçevesi inşa etmektir. Şekil 1’ de Cherubim’ in genel mimarisi görülmektedir.



Şekil 1- Cherubim Ajan Tabanlı Güvenlik Mimarisi [10]

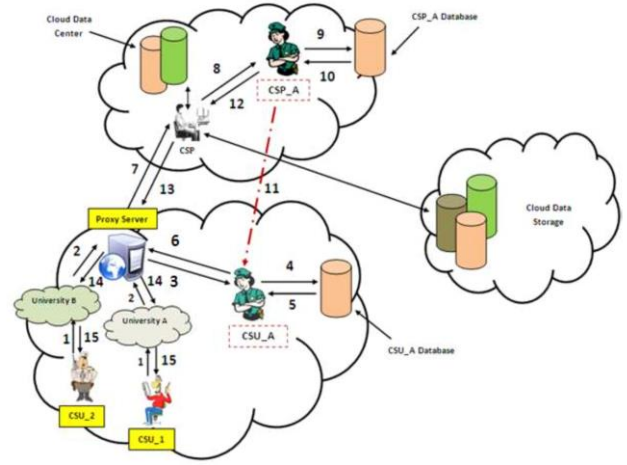
Mimaride görülen güvenlik ajanları bağlantısız durumlarda belirlenen güvenlik hedeflerini gerçekleştirmeye çalışır ve esnek bir yapıya sahiptir.

Ajan tabanlı diğer bir güvenlik mimarisi Seraphim 'in ana unsuru bir referans monitördür. Referans monitör, düğüm işletim sisteminin birlikte bulunduğu bir uzantı olarak uygulanır. Her düğüm, düğüm kaynaklarına yapılan tüm erişimlerin gerçekleştiği bir başvuru izleyicisine sahiptir. Politika çerçevesi referans monitörün bir parçasıdır. Politika çerçevesinin kendisi yeniden yapılandırılabilir ve gerektiğinde dinamik olarak yüklenebilir. Uygulamalar veya yöneticiler, erişim kontrolü politikası türünü ve erişim denetimi karar verme sürecinde kullanılan diğer kısıtlamaları kodlayan özelleştirilmiş bir kod parçası oluşturmak için, politika çerçevesi tarafından sağlanan arabirimi kullanır [14].



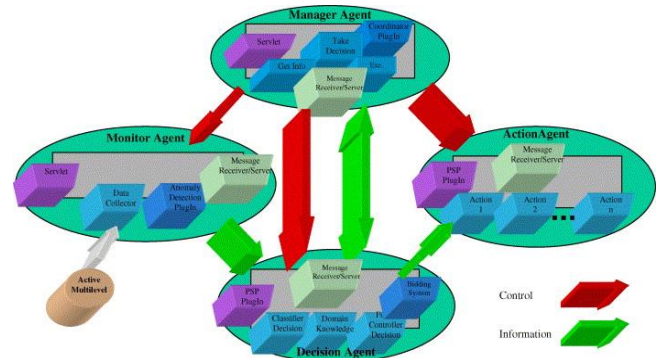
Şekil 2- Seraphim Ajan Tabanlı Güvenlik Mimarisi [14]

Bir diğer çalışmada WAY adlı bir ajan tabanlı güvenlik mimarisi bulut güvenliği için önerilmiştir. Şekil 3’ te bu mimari görülmektedir.



Şekil 3- WAY Ajan Tabanlı Güvenlik Mimarisi [16]

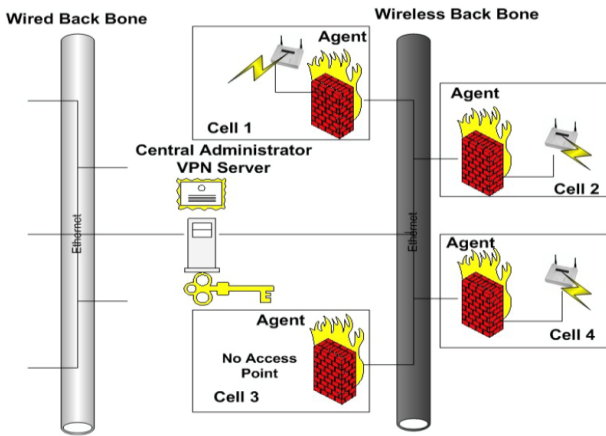
Dağıtık uygulamalar için geliştirilmiş anomalileri ve müdahaleleri güçlü bir şekilde saptamak için akıllı karar destek modülleri kullanan özerk bir aracı sistemi CIDS (Cougaar framework tabanlı saldırı tespit sistemi), bir güvenlik düğümünün dört farklı ajandan (yönetici ajanı, izleme ajanı, karar ajanı ve eylem ajanı) oluştuğu hiyerarşik bir güvenlik aracı çerçevesi sağlar. Bununla birlikte, bu ajanların faaliyetleri, müdahale ajanı aracılığıyla, algılama, iletişim kurma ve yanıt üretme sırasında koordine edilir. Her ajan, izlenen çevrenin çeşitli güvenlik sorunlarını çözmek için koordinasyon içinde benzersiz işlevler gerçekleştirir [17]. Şekil 4’ te CIDS mimarisi görülmektedir.



Şekil 4- CIDS Ajan Tabanlı Güvenlik Mimarisi [17]

Mohan K Chirumamilla ve Byrav Ramamurthy tarafından kablosuz yerel alan ağları için geliştirilmiş mimaride sahte erişim noktaları, kablosuz karışık düğümler ve yetkisiz istemciler gibi yetkisiz kablosuz öğelerin varlığını saptayan tamamen güvenli bir ajan tabanlı saldırı tespit sistemi tasarlanmış ve uygulanmıştır. Tespit edilen kablosuz unsurun türüne bağlı olarak, sistem buna göre tepki verecektir. Kablosuz unsurun sahte bir erişim noktası veya kablosuz karışık bir düğüm olması durumunda, yanıt coğrafi bilgi, öğe tespit edildiği zaman vb. ilgili bilgileri ilgili personele

gönderir. Kablosuz öge yetkisiz bir müşteri olduğu ortaya çıkarsa, yanıt, o istemcinin ağa girmesini engeller, böylece yetkisiz erişimi engeller [18]. Şekil 5’ te önerilen mimari bulunmaktadır.

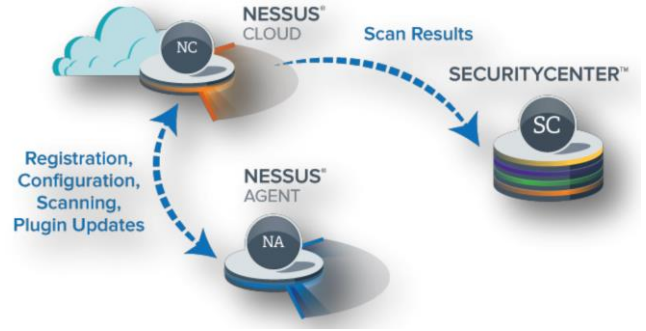


Şekil 5- Kablosuz Yerel Ağlar için Ajan Tabanlı Güvenlik Mimarisi [18]

Ajan tabanlı güvenlik mimarisi olarak 2002 yılında Allen Eugene Ott ve Frank Ernest Oldham tarafından ve 2004 yılında kabul edilen patentte ana bilgisayar seviyesindeki faaliyetleri tespit eden ve olayın oluştuğu olayları korunan ağa bağlı bir güvenlik sunucusuna raporlayan mobil algılayıcı ajanlarından yararlanan bir güvenlik sistemi tanımlanmıştır. Bu sistemde güvenlik sunucusu olay verilerini işler, ağın mevcut durumunu / risk durumunu değerlendirir ve şebekenin mevcut durumuna yanıt olarak ağdaki mobil algılayıcı ajanlar dağıtımını yönetir. Güvenlik sunucusu, nispeten soyut olan ana makine seviyesindeki etkinlik verilerini temel alarak bağlamsal olarak ilgili durum / risk verilerini elde etmek için akıllı veri füzyon teknikleri kullanmaktadır. Güvenlik sunucusu, belirli olayları izlemek, istemci bilgisayarlara yüklenmiş aktif mobil algılayıcı araçlarını geri çekilmek, mobil algılayıcı ajanları korumalı ağın içinde taşımak ve mobil algılayıcı ajanlara yön veren diğer yönetici ve düzenleyici eylemleri gerçekleştirmek için ek mobil algılayıcı ajanları dağıtabilir [15].

Bu buluşa uygun bir bilgisayar ağı güvenlik sistemi, bilinen güvenlik sistemlerine göre gelişmiş saldırılara karşı artan bir koruma seviyesi sağlar. Ağ güvenlik sistemi yanlış algılamaları azaltırken saldırı tespit oranlarını geliştirir. Ağ güvenliği sistemi, bilinen saldırı düzenlerine ve bilinmeyen saldırı yöntemlerine karşı koruma sağlayan uyarlamalı teknikler kullanır. Ayrıca, ağ güvenlik sistemi kolaylıkla yeniden yapılandırabilir ve güncellenebilir çünkü özelleştirilmiş yerel uygulamalara güvenmeniz gerekmez [15].

Nessus’ un ajan tabanlı güvenlik sisteminin mimarisi Şekil 6’ de görülmektedir.



Şekil 6- Nessus Ajan Tabanlı Güvenlik Sistemi [11]

Nessus Güvenlik Sistemi mimarisinde de ajanın bulut güvenlik merkezi ile bağlantı olması durumunda iletişime geçip sistem izleme bilgilerinin aktarıldığı, bağlantısız durumlarda ise belirlenen güvenlik hedeflerini gerçekleştirmek için sistemi izlediği görülmektedir. Qualy’ s Cloud Agent aynı mantıkla çalışan başka bir üründür.

#### IV. SONUÇLAR

Bu çalışmada ajan tabanlı güvenlik mimarileri incelenmiştir. Her mimari kendi belirlediği amaç fonksiyonları gerçekleştirmek için üretilmiş ajanlarla çalışmaktadır. Ajanların esneklikleri ve otonom çalışabilmeleri özelliğinden faydalanılarak kurulacak güvenlik sistemi mimarisinin amaç fonksiyonlar için esnek ve otonom yapıda olması sistemlerin daha güvenli ve güvenilir bir şekilde çalışmasına katkı sağlayacaktır.

#### REFERANSLAR

- [1] UK Ministry of Defence (MOD). The UK Approach to Unmanned Aircraft System: Joint Doctrine Note 2/11, 2012.
- [2] Williams, R. Autonomous Systems Overview. BAE Systems, 2008.
- [3] S Franklin, A Graesser, Is it an Agent, or just a Program?: A Taxonomy for Autonomous Agents Intelligent agents III agent theories, architectures, 1997 – Springer.
- [4] <http://www.crystaliz.com/logicware/mubot.html>
- [5] Stuart J. Russell and Peter Norvig. Artificial Intelligence: A Modern Approach. Prentice Hall, 1995.
- [6] Pattie Maes. Artificial Life Meets Entertainment: Life like Autonomous Agents. Communications of the ACM. (38):11, 108-114, 1995.
- [7] <http://activist.gpl.ibm.com/WhitePaper/ptc2.htm>
- [8] Tolks, A., and Uhrmacher, A.M. ‘Agents: Agenthood, Agent Architectures, and Agent Taxonomies’. In Agent-Directed Simulation and Systems Engineering, edited by Yılmaz and Ören, 75–109. Weinheim, Germany: Wiley-VCH, 2009.
- [9] <https://www.turkcebilgi.com/guvenlik>
- [10] Roy H. Campbell, and Tin Qian. Dynamic agent- based security architecture for mobile computers. In the Second International Conference on Parallel and Distributed Computing and Networks, Brisbane, Australia, December 1998.
- [11] [http://static.tenable.com/prod\\_docs/SC\\_5.1\\_with\\_Nessus\\_Agents.pdf](http://static.tenable.com/prod_docs/SC_5.1_with_Nessus_Agents.pdf)
- [12] Zhaoyu Liu, Prasad Naldurg, Seung Yi, Tin Qian, Roy H. Campbell, and M. Dennis Mickunas, An Agent Based Architecture for Supporting Application Level Security. DARPA Information Survivability Conference and Exposition, Hilton Head Island, South Carolina, January 2000.

- [13] Roy H. Campbell and M. Dennis Mickunas. Building dynamic interoperable security architecture for active networks. an accepted proposal to DARPA BAA9803, 1998.
- [14] Roy H. Campbell, Zhaoyu Liu, M. Dennis Mickunas, Prasad Naldurg, and Seung Yi, Seraphim: Dynamic Interoperable Security Architecture for Active Networks. IEEE Third Conference on Open Architectures and Network Programming Proceedings (OPENARCH'2000), Tel Aviv, Israel, March 2000.
- [15] Patent: A. Ott, F. Oldham, Computer network security system utilizing dynamic mobile sensor agents, 2004.
- [16] Shantanu Pal, Sunirmal Khatua, Nabendu Chaki, Sugata Sanyal, "A New Trusted and Collaborative Agent Based Approach for Ensuring Cloud Security," Annals of Faculty Engineering Hunedoara International Journal of Engineering (Archived copy), scheduled for publication in vol. 10, issue 1, January 2012. ISSN: 1584-2665.
- [17] Dasgupta, D., Gonzalez, F., Yallapu, K., Gomez, J. and Yarramsetii, R. CIDS: An agent-based intrusion detection system, Computers Security, Volume 24, Issue 5 , pp. 387-398, 2005.
- [18] M. K. Chirumanilla, B. Ramamurthy, " Agent Based Intrusion Detection and Response System for Wireless LANs ," IEEE International Conference on Communications, 2003. ICC '03.