Kablosuz Yerel Alan Ağlarında Yapay Bağışıklık Sistemi ile Saldırı Tespiti ve Performans Analizi

Erhan Akbal[1] Burhan Ergen[2]

[1] Enformatik Bölümü, Fırat Üniversitesi, Elazığ
[2]Bilgisayar Mühendisliği, Fırat Üniversitesi, Elazığ

[1]e-posta: erhanakbal@firat.edu.tr [2] e-posta: bergen@firat.edu.tr

Özetçe

Kablosuz ağ sistemlerinin hızla çoğalması ve mobil uygulamaların gelişmesi ağ güvenliğini tehdit edecek unsurların artmasına neden olmuştur. Ağı korumak için kullanılan güvenlik duvarları, virüs yazılımları ve koruyucu programlar uzun süre sistemi korumakta yeterli olmamaktadır. Bunun sebebi ise istenmeyen durumların sürekli artması ve bunlara karşı önlem alınmakta gecikilmesidir. Bizim amacımız bu yetersizliği ortadan kaldıracak yeteneğe sahip olan YBS ile kablosuz ağları ve ağ cihazlarını uzun süreli olarak herhangi bir müdahaleye gerek kalmadan ve performans kaybı yaşamadan oluşan istenmeyen durumları tespit etmek ve ağı korumaktır. Yaptığımız çalışmada kablosuz ağlarda saldırı tespitine farklı bir yönden yaklaşılarak tespit işlemi tüm kullanıcılar üzerinde yapmak yerine erişim noktası üzerinden kontrol işlemi gerçekleştirilmiş ve klasik yöntemlere göre daha hızlı ve daha performanslı sonuçlar elde edebilmektedir.

Anahtar Kelimeler: Kablosuz Alan Ağları, Yapay Bağışıklık Sistemleri, Saldırı Tespiti

1. Giriş

Saldırı tespit sistemleri saldırıyı tespit etme yöntemlerine göre birçok sınıfa ayrılmaktadır. Bu sistemlerden ağı en etkili ve en güvenli şekilde koruyabilme yeteneğine sahip olanlar zaman serileri kullanan sistemlerdir. Bu sistemlerin başında Yapay Bağışıklık Sistemleri gelmektedir. Yapay bağışıklık sistemleri insan vücudundaki antikorların mikrop ve mikroorganizmalara karşı vücudu koruması yaklaşımından ortaya çıkmıştır. Sistem rasgele detektörler üreterek ağda oluşan istenmeyen durumları tespit etme ve tekrar aynı durumlarla karşılaşması halinde otomatik yanıt verme yapısına göre çalışır.

Bağışıklık sistemi oldukça karmaşık bir yapıdadır ve çoğu araştırmacı bunun karmaşıklığını kabul etmektedir. Bağışıklık sisteminin öncelikli işi tanınan (self) durumlarla tanınmayan (nonself) durumları ayırt etmesidir. Bu durum birçok çalışmada ispat edilmiştir [1]. Kablosuz Yerel Alan Ağları ise WLAN (Wireless Local Area Networks), iki yönlü geniş bant veri iletişimi sağlayan, iletim ortamı olarak fiber optik veya bakır kablo yerine telsiz frekansı (Radio Frequency, RF) veya kızılötesi ışınları kullanan ve salon, bina veya yerleşke gibi sınırlı bir alanda çalışan iletişim ağlarıdır [3]. Sinyalin radyo frekansları ile kullanıcılara ulaştırılması kötü niyetli kişilerin ağa girmesini kolaylaştırmaktadır ve bu kablosuz ağlarda güvenliği önemli bir unsur olarak karşımıza çıkarmaktadır. Çalışmada böyle bir kablosuz ağ yapısına akıllı sistem uygulamalarından olan yapay bağışıklık sistemi adapte edilmiş ve elde edilen sonuçlar verilmiştir.

2. Kablosuz Ağlarda Bağışıklık Sisteminin Yapısı

Çalışmada uygulamalar kablosuz bir ağ üzerinde gerçekleştirilmiştir. Bilgisayar güvenlik sistemi bir bilgisayarı veya bir bilgisayar ağını izinsiz ve yetkisiz saldırılardan korumak zorundadır [2]. Burada insan bağışıklık sistemi nasıl insanı yabancı patojen saldırılarından koruma özelliğine sahipse, bilgisayar güvenlik sistemleri de bilgisayarları ya da bilgisayar ağını yabancı saldırılardan korumalıdır. Ayrıca bilgisayar güvenlik sistemi, sistemi içeriden gelebilecek ataklara, yazılım sorunlarına ve diğer iç hatalara karşı bilgisayarın normal toleranslarını göz önünde bulundurarak korumak zorundadır [5].

2.1. Kablosuz ağda tanımlanan normal durumlar

Uygulama ortamı olarak kablosuz (Wireless) ağ üzerinde iletişim halinde olan bilgisayarlar kullanılmıştır. Ağ standartları TCP/IP protokol kümesi ile oluşturulmuştur. TCP/IP protokol kümesi internet üzerinden bilgisayarların veri alıp göndermesini sağlayan birçok protokol içermektedir. Sistemde TCP/IP bağlantılarının karakteristik özellikleri kullanılarak bir veri yapısı çıkarılmıştır. Bu veri yapısı içerisinde TCP/IP standartları gereği kaynak adresi, hedef adresi port numarası ve iletişim bayrak bilgileri bulunmaktadır. Ağ üzerindeki TCP/IP veri paketleri binary stringler haline getirilmiştir. Bir kablosuz ağda oluşabilecek tüm normal durumlar tanınan durumlar kümesini, bunun dışındakiler ise tanınmayan durumlar kümesini oluşturmaktadır [4].
Normal kablolu networklarda ağ üzerindeki paketler tüm kullanıcılara ulaşamamaktadır. Daha önce yapılan uygulamalarda kablolu ağlar kullanılmış ve incelenen trafik sadece aynı vlan (virtual local area network) içerisindeki bilgisayarlardır. Fakat kablosuz ağlarda radyo dalgalarını yayan erişim noktası kablosuz ağa dahil olan tüm kullanıcılara veri paketlerini iletmektedir ve ağa dahil olmayan bilgisayarlarda veri paketlerine ulaşabilmektedir bu da daha tehlikeli bir ortam oluşturmaktadır. Erişim noktası üzerinden yapılan kontrol işlemi ile tüm durumların kontrol edilmesi sağlanmış ve tespit işleminin başarısı ve performansı arttırılmıştır.

2.2. Tespit İşlemi ve Yeniden Algılama

Negatif seçim algoritmamızda detektörler olgunlaşma süresi boyunca ayrıntılı bir şekilde incelenmektedir. Olgunlaşma süreci boyunca çeşitli problemler ile karşılaşılmaktadır. Bu problem normal tanınan durumların olağan değişimleridir.

Kablosuz ağa bir bilgisayar eklendiğinde çıkarıldığında veya ağa yeni bir kullanıcı dahil olup çıktığında yada yeni bir yazılım yüklendiği zaman normal olarak tanınmakta olan durumlar kümesi değişmektedir [6]. Çünkü önceden tanımlanan durumlar kümesi ile arasında farklılıklar oluşacaktır. Bu tanınan durumlar kümesinin değişiklik göstermesi yanlış alarmlara sebep olur ve otomatik bağışıklık tepkileri için istenmeyen bir durumdur. Yanlış alarmların oluşmasını engellemek için insan vücudunda çeşitli mekanizmalar bulunmaktadır. Bu mekanizma insan vücudunda T yardımcı hücrelerinden zorunlu taşıyıcı B hücrelerinin uyarılmasına benzemektedir. Burada olgunlaşan detektörler yirmi dört saat süre boyunca eşleşmeye uğramaktadır ve bu eşleşme sonucu bir uyarı sinyali alınmazsa bu detektör sistemden çıkarılmaktadır. Sonuçta yanlış alarma sebep olan detektörler sistemden böylelikle çıkarılacaktır ve hataları ortadan kaldırmaktadır [7]. İnsanlarda doğru alarmlar elde etmek için ise çeşitli incelemeler yapılmaktadır. Bu işlem tanınan durumlar kümesini geliştirmek ya da gelişimlerini tamamlamaları için sisteme bir kazanç sağlamaktadır. Tahmini doğal bağışıklık sistemi uyarmaları ile benzerdir. Bu özellik faydasının yanı sıra potansiyel uygun olmayan mutasyonlara karşıda koruyucu bir etkiye sahiptir.

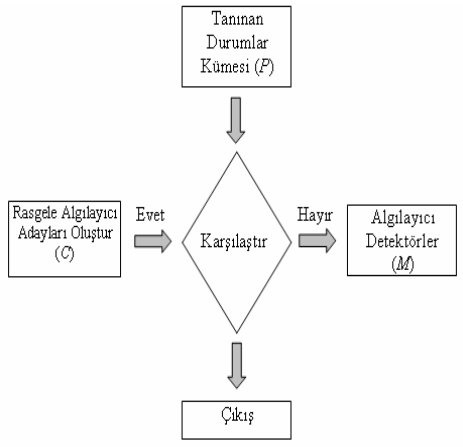
Algılama işlemi için sistemdeki her bir anormal durum için bir detektör kullanılmalıdır [9]. Bu da iyi bir tespit işlemi için birçok detektör gerekliliğini ortaya çıkarır. Algılama işleminin tek bir detektörle yapılması en genel durumdur ve sadece teoriktir. Çünkü sistem aynı anda birçok normal özellikli farklı durumla karşılaşabilmektedir. Örneğin kablosuz ağa yapılan saldırı, hem sinyalin kapsadığı alan içindeki bir bilgisayardan ya da internet ortamından bağlanan herhangi bir bilgisayardan gerçekleşebilir. Kablosuz ağın kapsama alanı içerisindeki bilgisayarlar aynı ağa dahildir ve birbirleriyle direk iletişim halindedir. Bunun dışındaki iletişimler internet üzerinden veri transferi yolu ile gerçekleşmektedir. Böyle bir duruma karşı önlem almak içinde birden fazla detektör kullanılmasına ihtiyaç vardır. İnsan vücudunda da aynı şekilde vücut içerisinde aynı anda dolaşan birçok detektör bulunmaktadır. İnsan vücuduna aynı anda birçok patojen saldırı gerçekleşmesi halinde farklı detektörler bu saldırılara karşı cevap vermektedir [10]. Burada detektör sayısının fazla olması tanınan durumların daha fazla olacağı anlamına gelmektedir.

Sistemdeki detektörlerin belirli yaşam süreleri bulunmaktadır. Bu yaşam süreleri sonunda detektörler ya hafıza hücrelerine dönüşür ya da öldürülmektedir. İnsan vücudunda da aynı şekilde detektörler ya hafıza hücrelerine dönüşmekte ya da doğal öldürücü hücreler ile öldürülüp sistemden kaldırılmaktadır.

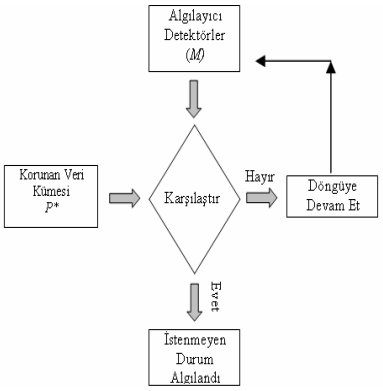
Hafıza hücreleri uzun süreler hayatta kalır ve kan, lenf ve lenfoid organlarda aktif olarak dolaşım halinde bulunurlar. Hafıza hücrelerinin Antijenler tarafından uyarılması, ikincil Antijen yanıtlarının oluşmasına neden olur [11]. İkincil yanıtlar hem süre hem de miktar bakımından ilk bağışıklık yanıtından daha etkindirler. Buda kablosuz ağa olabilecek aynı özellikteki bir başka saldırıya karşı çabuk ve hızlı bir uyarı vermesini sağlar

2.3. Ağ tabanlı negatif seçim algoritması yapısı

Öncelikle, korunacak durumların kümesi belirlenir ve *'self-set'*(P) olarak adlandırılır. Bu küme ağın normal durumlarını kapsamaktadır. Normal durumlar ağ üzerindeki band genişliği, hangi portların kullanılacağı gibi bilgileri içermektedir. Negatif seçim algoritmasına dayanarak, 'self-set' kümesine ait olmayan elemanları tanımakla sorumlu bir algılayıcılar *(detektörler)* (M) kümesi oluşturulur. Negatif seçim algoritmasının çalışma yöntemi akış diyagramı olarak şekil 1'de verilmiştir [8].



a) Detektör Kümesi Oluşturma İşlemi



b) Normal Olmayan Durum Tespiti

Şekil 1. Negatif Seçim Algoritması

3. Doğal bağışıklık sistemi ile tespit sisteminin eşleşmesi

Doğal bağışıklık sisteminde kullanılan insan vücudu, tanınan hücreler, tanınmayan hücreler, antijen, antijen yapısı, antikor, negatif ve pozitif seçim gibi parametreler yapay bağışıklık sisteminde de kullanılmıştır ve bunların karşılıkları mevcuttur [12].

İnsan Vücudu: Kablosuz ağı oluşturan tüm elemanlar

Vücudun Tanıdığı Hücreler: Ağ içerisindeki normal durumların her biri.

Vücudun Tanımadığı Hücreler: Ağ içerisinde normal olmayan durumların her biri.

Antijen: Sisteme zarar vermek üzere yada sistemde tehlike oluşturan veri paketlerinin her biri.

Antikor: Sistemde rasgele olarak oluşturulur ve istenmeyen durumların tespitini sağlar. Binary olarak ifade edilir. Yapısında hedef ip adresi, kaynak ip adresi, hedef port, kaynak port ve paketin cinsini belirten bir bitten ifade edilir.
Negatif Seçim: Sistemde istenmeyen ve zararlı olan paketleri ayırt edilmesi, tanınmayan durumların hafıza hücrelerine kaydedilmesi için gereklidir.

3.1 Çaprazlama ve Karşılaştırma İşlemi

Karşılaştırma işlemi yapılabilmesi için sistem üzerindeki paketler Tablo 1 e göre yapılandırılmıştır. Tabloda paketlerin durumları harflerle ifade edilmiştir.

Tablo 1 – *Durumların alfabetik gösterimi [8]*

A=RREQ gönderildi
B=RREP gönderildi
C=RERR gönderildi
D=DATA gönderildi ve izlenen düğüme gitmeyen kaynak IP adresi
E=RREQ alındı
F=RREP alındı
G=RERR alındı
H=DATA alındı izlenen düğüme gitmeyen Hedef IP adresi

İlk olarak verilen basit alfabetik yapıya göre bir bitsel veri yapısı oluşturulursa aşağıdaki şekilde elde edilir;

I_1 = (EAFBHHEDEBHDHDHHDHD,…)

İkinci olarak gen yapıları tanımlanır. Çünkü eşleştirme işleminde kullanılacak en küçük yapı gendir [8].

Gen1=#E
Gen2=#(E*(A veya B))
Gen3=#H
Gen4=#(H*D)

Buradaki genler alfabetik olarak ifade edilmiştir. #(E*(A veya B)) ifadenin anlamı genlerin E ile başlayacağı ve uzunluğu iki ya da üç etiket ile ifade edilebilir. Gen E ile başlar A veya B ile sonlanır.
I_1 geni I_2 genini oluşturmak için kullanılabilir ve aşağıdaki yapı elde edilir.

I_2 = (3 2 7 6)
Bit eşleştirmesini kolaylaştırmak için antijeni 1 ler ve 0 lardan ifade edebiliriz. Örneğin I_2 antijenini aşağıdaki gibi gösterebiliriz [12].

I_3=(0000001000 0000000100 0010000000 0001000000)

Sonuçta I_3 antijeni basit bir antijen yapısını göstermektedir. I_3 antijeni 10 bit ile ifade edilmiştir ve bu standart değer olarak kabul edilmiştir. Antikorlarda antijene benzer bir yapıya sahiptir. Fakat antikorlar antijenlerden farklı olarak birçok antijeni aynı anda tanıma özelliğine sahip olacağından daha çok özellik içermektedir. Yaptığımız çalışmada bir antijene karşılık bir antikor görev yapmaktadır. Fakat antikor tüm durumları kapsayacak şekilde tanımlanmıştır. Antijenin olabilecek her pozisyonu karşılamaktadır.
Örnek olarak antikor:

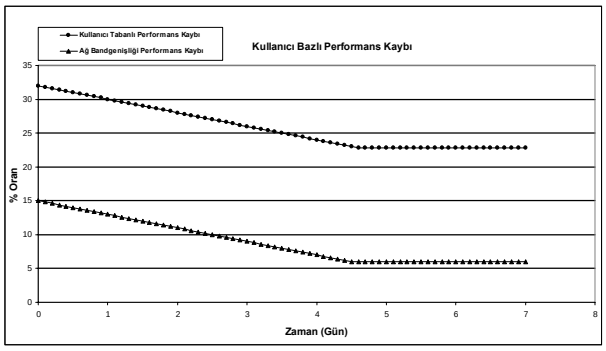
a_1 = (1100001001 1000010110 0011001000 1001000100)

verilen a1 antikoru I_3 antijenini eşleşebilmektedir çünkü I_3 de olabilecek tüm durumları kapsamaktadır [12].

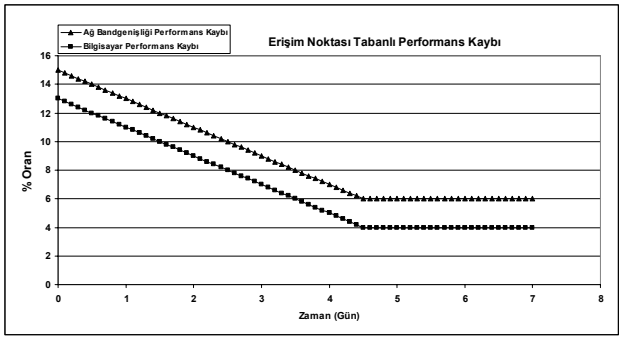
4. Uygulama Sonuçları

Uygulama ortamında tanımlanan yapıya göre sistem çalıştırılmıştır. Daha önceki çalışmalarımızda sistem 7 gün süre ile gözlenmiş bu süre içerisindeki sonuçlar değerlendirilmiştir. Bu çalışmamızda uygulama 21 gün süre ile çalıştırılmış ve log kayıtları tutulmuştur. Burada ulaşmaya çalıştığımız sonuç yapay bağışıklık sisteminin ağı uzun süreler boyunca performans kayıplarına uğramadan doğru bir şekilde koruyup korumayacağını tespit etmektir. Elde etiğimiz sonuçlara göre uygulamanın çalışma süresi arttıkça doğru tespit oranları da artmaktadır. Fakat buna bağlı olarak uzun süre çalışan kullanıcı bilgisayarlarının performansları düşmektedir. Bunun sebebinin YBS uygulamasından çok bilgisayarların olağan performans kayıpları olduğunu düşünmekteyiz. Tespit programının bilgisayarı meşgul etme oranlarında önemli bir değişiklik gözlenmemiştir. Şekil 2 ve Şekil 3'de verilen grafiklerde bunlar gösterilmektedir. Sistemin değerlendirilmesi yapılırken aşağıdaki ölçütler kullanılmıştır.

Performans Ölçütleri: Uygulama sonuçlarını değerlendirme kriterleri aşağıdaki ölçütlere göre yapılmıştır. [11].
Ağın Band genişliği kaybı: Ağ üzerindeki çalışan uygulamanın ağın band genişliğini meşgul etme oranı
Kullanıcı Performans Kaybı: Uygulamanın çalıştırıldığı ağ bilgisayarlarının işlemci ve belleklerindeki performans kaybı



Şekil 2. Kullanıcı tabanlı YBS



Şekil 3. Erişim noktası tabanlı YBS

Sistem Δt=21 gün süre ile gözlenmiştir. İzleme süresi boyunca değerler gün içerisinde 6 saatte bir alınmıştır. Erişim noktası üzerinden gerçekleştirilen uygulama ile ağ trafiğinin tümü izlendiği için daha fazla paket trafiği üzerinden tespit işlemi gerçekleştirilmiş ve daha doğru tespit oranları elde edilmiştir. Şekil 3' de verilen grafikte erişim noktası tabanlı YBS ile daha doğru tespit oranları elde edildiği gösterilmektedir. Bunun sebebinin erişim noktası ile paket trafiğine daha fazla hakim olması ve YBS nin daha fazla durumu gözleyerek tanıdığı durumları arttırmasından kaynaklandığı sonucuna varılmıştır. Uygulama sonucunda kullanıcı bilgisayarlarında performans kayıpları gözlenmiştir fakat daha önce belirtildiği gibi bu kayıpların olağan performans kayıpları olduğu görülmüştür.

5. Sonuç

Yapılan çalışmada, yapay bağışıklık sisteminin kablosuz ağlarda farklı bir uygulaması üzerinde durulmuştur. Yapılan uygulamalardan farklı olarak kullanıcı tabanlı yerine ağ tabanlı YBS uygulanmıştır. Ağ tabanlı ve kullanıcı tabanlı YBS uygulanmasının bilgisayarları ve ağı meşgul etme oranlarına bakılmıştır. Saldırı tespitinin önemli olmasının yanında bilgisayarların ve ağında performanslı bir şekilde çalışması önemli bir kriterdir. YBS nin uygulanma farklılığına göre ağdaki ve bilgisayarlardaki performansı değiştirdiği görülmüştür. Kullanıcı tabanlı YBS de kullanıcıların bilgisayarlarında önemli oranda performans düşüklüğü gözlenmiştir. Bunun yanında ağ performans düşüş oranları izlenmiştir. Ağ tabanlı YBS uygulamasında ise kullanıcı bilgisayarlarında çok büyük performans kaybı olmadığı görülmüştür. Ağ tabanlı ve kullanıcı tabanlı YBS nin ağ performans kaybı oranlarına bakıldığında aralarında çok büyük bir farkın olmadığı görülmüştür. Bunun sebebi olarak ağ üzerindeki paket trafiğinde herhangi bir değişikliğin olmamasıdır. Ağ tabanlı ve kullanıcı tabanlı uygulamanın her ikisinde de ağ üzerindeki paketler tüm kullanıcılara ve erişim noktasına ulaşmaktadır. Bu sebeple erişim noktası üzerinden YBS uygulanması daha performanslı olduğu sonucu ortaya çıkmıştır.

6. Teşekkür

Bu çalışma Fırat Üniversitesi Bilimsel Araştırma Projeleri (FUBAP) tarafından 1167 proje numarası ile desteklenmektedir.

7. Kaynakça

[1] Buchegger, S. and Le Boudec, J.-Y.. A Robust Reputation System for Mobile ad hoc Networks Technical Report, *EPFL-DI-ICA, Lausanne*, Switzerland, Temmuz 2003.

[2] S.Buchegger ve J.,Y. Le Boudec, "Performance Analysis of the CONFIDANT protocol: Cooperation of nodes - Fairness In Distributed Ad-Hoc Networks", In *of IEEE/ACM Symposium on Mobile Ad-Hoc Networking and Computing (MobiHOC)*, Lausanne, CH, Haziran 2002.

[3] S. Buchegger ve J.-Y. Le Boudec, "The Effect of Rumor Spreading in Reputation Systems for Mobile Ad-hoc Networks", In *Proceedings of WiOpt `03: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks.*, Sophia-Antipolis, France, Mart 2003.

[4] Forest.S., Hofmeyr. S. A. "Immunology as Information Processing. Design Principles for Immune System & Other Distributed Autonomous Systems", L.A. Segel and I. R. Cohen, eds. *Oxford Univ. Pres*. 2000

[5] Kim, J. and Bentley, P. J., Evaluating Negative Selection in an Artificial Immune System for Network Intrusion Detection, Genetic and Evolutionary Computation Conference 2001 (GECCO-2001), San Francisco, 1330 – 1337, 2001

[6] Zhang, Y., Lee, W., ve Huang, Y., "Intrusion Detection Techniques for Mobile Wireless Networks", *Wireless Networks Vol 9*, 2003, sf: 545-556.

[7] De Castro, L.N. ve Von Zuben F.J., "The Clonal Selection Algorithm with Engineering Applications", *GECCO 2000*, Las Vegas, Nevada, USA, 2000.

[8] Sarafijanovic, S. ve Le Boudec, J.Y., "An Artificial Immune System Approach with Secondary Response for Misbehavior Detection in Mobile Ad-Hoc Networks" *Tech Report IC/2003/65, EPFL-DI-ICA, Lausanne*, Switzerland, Kasım 2003.

[9] Kenneth S. Edge, Gary B. Lamont, and Richard A. Raines, "Multi-objective Mobile Network Anomaly Intrusion", Air *Force Institute of Technology, Dayton, OH, USA,* 2006

[10] S. Buchegger, Cedric Tissieres, J. Y. Le Boudec, "A Test-Bed for Misbehavior Detection in Mobile Ad-hoc Networks", *How Much Can Watchdogs Really Do? Technical report*, No. IC/2003/72, Kasım 2003.

[11] Le Boudec, J. Y. ve Sarafijanovic ,S., "An Artificial Immune System Approach to Misbehavior Detection in Mobile Ad-Hoc Networks" *Proceedings of Bio-ADIT 2004*, Lausanne, Switzerland, Ocak 2004

[12] Sarafijanovic, S. ve Boudec, J., "An Artificial Immune System for Misbehavior Detection in Mobile Ad-Hoc Networks with Virtual Thymus, Clustering, Danger Signal, and Memory Detectors". *International Journal of Unconventional Computing*, Vol 1, Feb 2005, sf: 221-254.

[13] Patwardhan, A. Parker, J., Joshi,A., Karygiannis, A., ve Iorga,M. "Secure Routing and Intrusion Detection in Ad Hoc Networks", *Third IEEE International Conference on Pervasive Computing and Communications*, Kauai Island, Hawaii, 2005.

[14] Akbal, E., Ergen, B., "A Performance Comparison of User and Access Point based Artificial Immune Systems for intrusion detection on a Wireless Local Area Network", International Journal of Computer Science and Network Security (IJCSNS), Vol 7, Mayıs 2007, sf: 119-124