Güvenlik Duvarları için Politika Anomali Belirleme Algoritmasının Deneysel Uygulaması

Füsun ÇETİN, Oğuz YARIMTEPE, Tuğkan TUĞLULAR
İzmir Yüksek Teknoloji Enstitüsü, Bilgisayar Mühendisliği Bölümü, İzmir
fusuncetin@iyte.edu.tr, oguzyarimtepe@iyte.edu.tr, tugkantuglular@iyte.edu.tr

Özet: Güvenlik duvarı, iç ağı dış ağdan gelebilecek saldırılara karşı koruyan bir yazılım ya da donanımdır. Güvenlik duvarının işlevselliği filtreleme kurallarına ve bu kuralların sırasına bağlıdır. Doğru kural sırasını belirlemek için kurallar arasındaki bütün matematiksel ilişkiler dikkate alınmalıdır. Tek ve dağıtık güvenlik duvarı ortamları için anomali bulma algoritmaları "Politika Anomali Belirleyicisi" adı verilen bir yazılım aracında uygulanmıştır. Bu algoritmaların işletim değerlerinin belirlenmesi için farklı kural setleri ve ağ yapıları kullanılarak testler yapılmıştır.

Anahtar Kelimeler: Güvenlik Duvarları, Güvenlik Duvarı Politikaları, Politika Anomali Belirleme.

Experimental Application Of Policy Anomaly Detection Algorithm For Firewalls

Abstract: Firewall is a software and/or hardware used to protect the inner network from attacks which may come from outer network. Firewall functionality depends on the filtering rules and their order. All rule relations must be considered in order to determine correct rule order. Anomaly detection algorithms are implemented for single and distributed firewall environments in a software tool called "Policy Anomaly Checker". A number of tests are performed using different policies and network topologies in order to obtain operational values of these algorithms.

Keywords: Firewalls, Firewall Policies, Policy Anomaly Detection.

1. Giriş

Güvenlik duvarları ağ güvenliğinde temel elemanlardan biridir. İnternet'in bir çok tehlikesi güvenlik duvarları sayesinde engellenebilir. Güvenlik duvarı bir iç ağın bir dış ağa bağlandığı noktaya kurulur ve iç ağa gelen ya da iç ağdan giden kabul edilmeyen trafiği paket bazında filtreler [1]. Filtreleme sıralı kurallar dahilinde gerçekleştirilir. Güvenlik duvarının doğru çalışması filtreleme kurallarına bağlıdır [2].

Sistem veya güvenlik yöneticileri doğru kural sıralamasını belirlemek için kurallar arasındaki matematiksel ilişkileri dikkate almalıdır. Filtreleme kurallarının sayısındaki artış güvenlik duvarı politikasındaki anomali oluşturma potensiyelini arttırır. Tek güvenlik duvarı ortamında politika, aynı paketin birden fazla filtreleme kuralına uyduğu güvenlik duvarı içi anomalileri içerebilir. Dağıtık güvenlik duvarı ortamında ise, aynı patika üzerindeki güvenlik duvarlarının aynı trafik üzerinde farklı filtreleme eylemleri gösterdiği durumlarda güvenlik duvarları arası anomaliler ortaya çıkabilir.

Bu çalışmanın amacı tek ve dağıtık güvenlik duvarları ortamında politika anomalilerini raporlamak için anomali belirleme algoritmalarını [3] uygulamaktır. Anılan algoritmalara ilişkin yaklaşım Bölüm 2'de anlatılmıştır. Bu algoritmalar Java programlama dili kullanılarak "Politika Anomali Belirleyicisi" adı verilen bir yazılım aracında uygulanmıştır. Bölüm

3'de bu yazılıma ait tasarım ve uygulama detayları verilmiştir. Bölüm 4 benzer çalışmalarda yapılmış deneylerle bu çalışmanın deneylerinin karşılaştırıldığı bölümdür. Takip eden bölümde ise literatürde bulunmayan deney sonuçları ortaya konmuştur. Gelecekte yapılabilecek çalışmalar sonuç bölümünde açıklanmıştır.

2. Politika Anomali Belirleme

Güvenlik duvarı politika anomalilerin belirlenebilmesi için kurallar arasındaki matematiksel ilişkilerin tespit edilmesi gereklidir. Bu ilişkiler kullanılarak güvenlik duvarı içi ve güvenlik duvarları arası politika anomalileri sınıflandırılabilir. Güvenlik duvarı içi politika anomalileri dört sınıfa ayrılır; gölgeleme anomalisi, genelleme anomalisi, fazlalık anomalisi ve bağıntı anomalisi. Güvenlik duvarları arası politika anomalileri ise yine dört sınıfa ayrılır; gölgeleme anomalisi, sahtelik anomalisi, fazlalık anomalisi ve bağıntı anomalisi [3]. Politika anomali belirleme algoritmalarını uygulamak için filtreleme kurallarının ağaç şeklinde gösterimi kullanılmıştır.

Politika anomalilerinin belirlenmesin-de güvenlik duvarı içi ve güvenlik duvarları arası ortamlar için algoritmalar geliştirilmiştir [4]. Güvenlik duvarı içi anomali belirleme algoritmasında temel fikir, politika ağacı kurulurken kurallar arasındaki anomalilerin tespit edilmesidir. Anılan algoritma özyinelemeli olarak çalışır. Politika içindeki her bir kuralın alanları kendisinden önce gelen kuralların ilgili alanları ile karşılaştırılarak kurallar arasındaki matematiksel ilişkiler tespit edilir. Tespit edilen ilişkiler yardımı ile kuralların eylem alanları karşılaştırılarak anomali tipleri belirlenir. Örneğin K_x ve K_y sırası ile aynı politika içindeki iki kural olduğu düşünüldüğünde eğer K_y kuralındaki bütün alanlar K_x kuralındaki bütün alanların eşiti ya da alt kümesi ise ve iki kuralın eylem alanları farklı ise bu iki kural arasında gölgeleme anomalisi vardır.

Güvenlik duvarları arası anomali belirleme algoritmasında anomali belirleme işlemi, ağ içindeki iki alt alanı birbirine bağlayan patikalar üzerindeki tüm güvenlik duvarları için gerçekleştirilmelidir. Algoritma işletilmeden önce alt ağlar arasındaki bütün patikalar belirlenir. Patika üzerindeki her bir güvenlik duvarı için ilk önce güvenlik duvarı içi anomali belirleme algoritması işletilir. Daha sonra belirlenen her bir yol için akışın kaynağına yakın olan güvenlik duvarının kuralları, güvenlik duvarı içi anomali belirleme algoritması kullanılarak politika ağacına yerleştirilir. Yol üzerindeki diğer güvenlik duvarlarının kuralları bu ağaç üzerine eklenerek kurallar arasındaki anomaliler tespit edilir.

3. Tasarım ve Uygulama

Güvenlik duvarının işlevselliği filtreleme kurallarına ve kuralların sırasına bağlıdır. Bu bölümde Politika Anomali Belirleyicisinin (PAB) tasarım ve uygulaması açıklanacaktır. Politika Anomali Belirleyici-sinin iki temel işlevselliği vardır:

Güvenlik duvarı içi anomali belirleme: Bu işlevsellikte seçilen politkanın kuralları arasındaki anomaliler belirlenir. Önceden tanımlanmış olan ağ topolojisindeki bir güvenlik duvarına ait politika seçilerek işlem gerçekleştirilir.

Girdi: Seçilen politika.
İşlem: Güvenlik duvarı politikası denetlenir.
Çıktı: Anomaliler.

Güvenlik duvarları arası anomali belirleme: Bir patika üzerinde var olan bütün politikalarda bulunan kurallar arasındaki anomaliler belirlenir. Bu işlevselliğin sağlana-bilmesi için ağlar ve altağlar arasındaki patikaların önceden bilinmesi gereklidir. Tanımlanmış olan

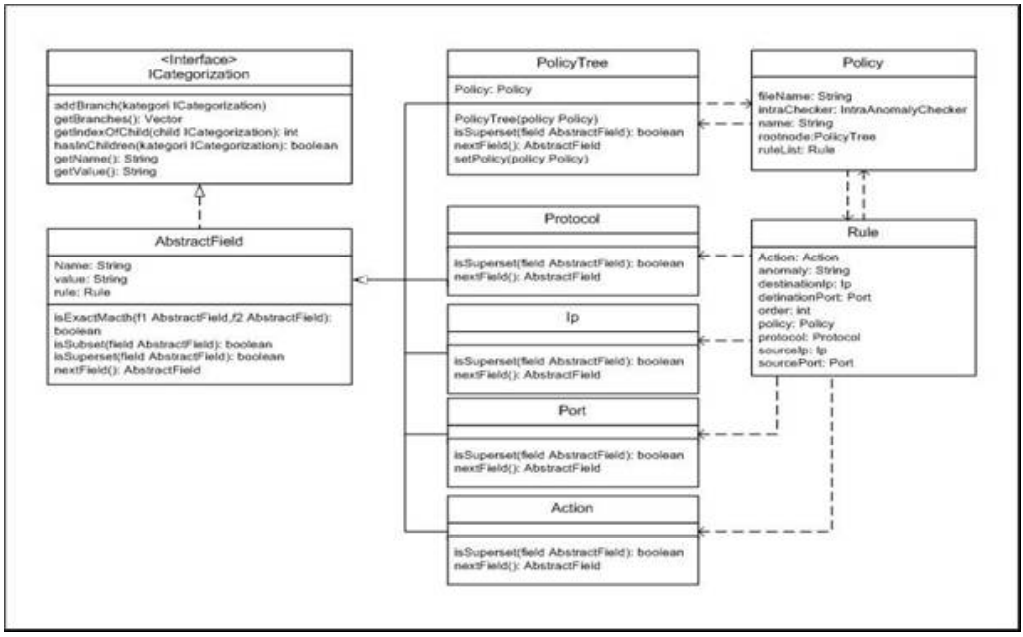
ağ topolojisindeki bir patika seçilerek işlem gerçekleştirilir.

Girdi: Seçilen patikanın politikaları.
İşlem: Patika politikaları denetlenir.
Çıktı: Anomaliler.

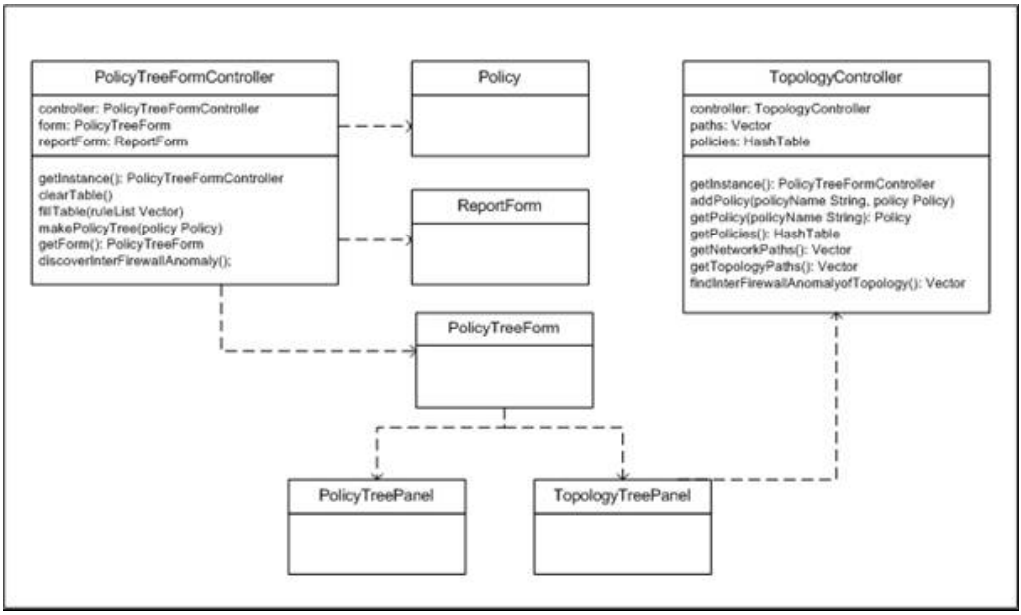
PAB nesneye dayalı tasarım metodları kullanılarak geliştirilmiştir. Nesneye dayalı tasarım; yazılımın yeniden kullanabilirlik, genişletilebilirlik ve güvenilirliğini sağlamak amacı ile kullanılır. Kalıtım, soyutlama, sarmalama ve çokyüzlülük nesneye dayalı tasarımın ana kavramlarıdır. Tasarım sürecinde nesneye dayalı kavramlara ek olarak tasarım şablonları da kullanılmıştır. Tasarım şablonları belirli yazılım sorunları üzerinde önceden belirlenmiş, tekrarlanabilir çözümlerdir.

PAB mimarisi üç katmandan oluşur. Kullanıcı arayüzü katmanı diğer katmanların üstündedir ve verilerin kullanıcıya gösteriminden sorumludur. Servis katmanı uygulama için iş kurallarının yerine getiril-mesinden sorumludur. Anomali belirleme algoritmaları bu katmanda uygulanmıştır. İçerik katmanı ise iş içeriğinin sunulmasından sorumludur.

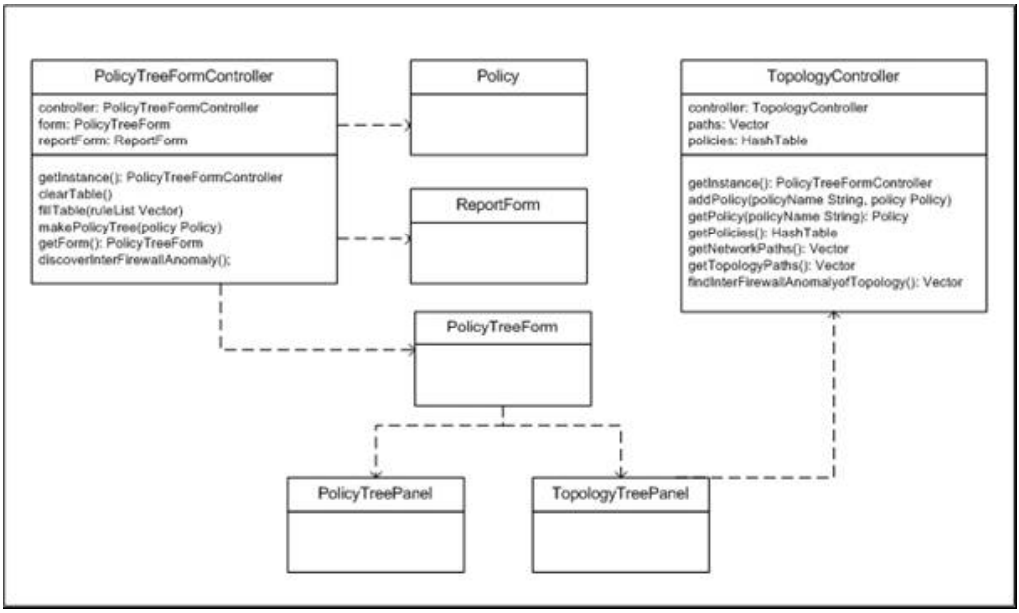
İçerik katmanı iş içeriğinin gösteriminden sorumludur (bkz. Şekil 1). Bir politika kurallardan ve kuralların ağaç gösteriminden oluşmaktadır. Politika aynı zamanda anomali denetleyicisini de içermektedir. Her kuralın <order, protocol, src_ip, dest_ip, src_port, dest_port, action> alanları vardır. *ICategorization* adı verilen interface sınıf, politika içindeki kuralların ağaç gösterimi için gerekli olan metodları sağlar. *AbstractField* adı verilen abstract sınıf ise kurallar arasındaki ilişkilerin belirlenmesini sağlayan metodları içerir.



Şekil 1. Politika Anomali Belirleyicisi İçerik Katmanı



Şekil 2. Politika Anomali Belirleyicisi Servis Katmanı



Şekil 3. Politika Anomali Belirleyicisi Kullanıcı Arayüzü Katmanı

Uygulamanın servis katmanı, iş kurallarının yerine getirilmesi için tasarlanmıştır (bkz. Şekil 2). *AnomalyChecker* adı verilen abstract sınıf, güvenlik duvarı içi ve güvenlik duvarları arası anomalilerin belirlenmesi için metodları içerir. Kullanıcı arayüzü katmanı politika ve topoloji ağaçlarının gösterimi için tasarlanmıştır (bkz. Şekil 3). *PolicyTreeForm-Controller* ve *TopologyController* adı verilen iki singleton sınıf ağ topolojisinden belirlenen patikayı kullanarak politikaları yaratır. Güvenlik duvarları arası anomalilerin belirlenmesi için politikaların sistemde tanımlı olması gerekmektedir. *ReportForm* sınıfı ise anomali belirleme işleminin sonuçlarının gösterimi için kullanılır.

Politika Anomali Belirleyicisinde iki temel senaryo vardır. İlk senaryo, güvenlik duvarı içi anomali belirleme senaryosudur. Kullanıcı uygulamanın arayüzünden "Discover Intra-firewall Anomaly" menüsünü seçtiğinde ilk olarak *TopologyController* sınıfından ilgili politika nesnesi çekilir ve politika ağacı arayüzde görüntülenir. Eğer politika ağacı daha önce kurulmamışsa politika ağacını kurmak ve anomali sonuçlarını almak için *IntraAnomalyChecker* nesnesi kullanılır.

İkinci senaryo güvenlik duvarları arası anomali belirleme senaryosudur. Kullanıcı uygulamanın arayüzünden "Discover Inter-firewall Anomaly" menüsünü seçtiğinde ilk olarak *TopologyController* sınıfından patikalar çekilir. Her bir patika için bu patika üzerinde kurulmuş güvenlik duvarlarının politikaları *TopologyController* sınıfından alınır. *InterAnomalyChecker* nesnesi de bu politikalar arasındaki anomalileri belirler.

4. Karşılaştırmalı Deneyler

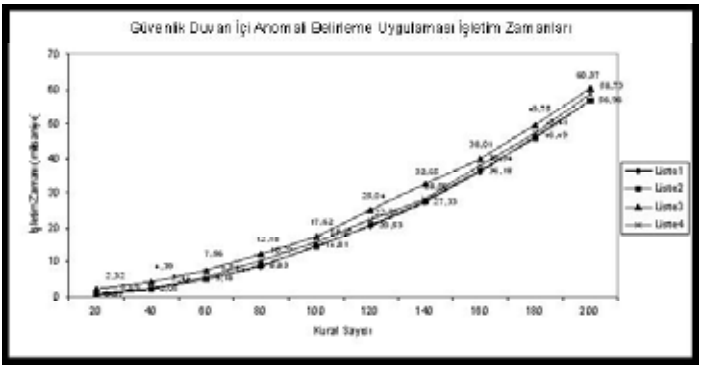
Güvenlik duvarı içi ve güvenlik duvarları arası anomali bulma algoritmalarının işletimsel değerlerini tespit etmek üzere farklı politikalar ve ağ topolojileri kullanılarak testler yapılmıştır. Bu testler Pentium IV-M 1.73 GHz. ve 1.49 GByte RAM olan bir bilgisayar üzerinde gerçekleştirilmiştir.

Güvenlik duvarı içi anomali belirleme algoritmasının işletimsel değerlerinin tespit edilmesi için dört kural listesi üretilmiştir. İlk liste yalnızca hedef adresleri farklı kurallar içerirken, ikince liste yalnızca kaynak adresleri farklı kuralları içermektedir. Bu iki liste en iyi durum senaryosudur çünkü her bir kuralın analiz edilmesi için minimum ağaç dolaşımı gerekmektedir. Üçüncü liste, her bir kural bir önceki kuralın üst kümesi olacak şekilde oluşturulmuştur. Bu liste en kötü durum senaryosudur çünkü her bir kural için ağacın tamamının dolaşılması gerekmektedir. Dördüncü listenin ortalama durum senaryosunu oluşturması için önceki üç listeden rastgele seçilen kurallar kullanılmıştır. Bu dört listenin oluşturulma mantığı [4]'den alınmıştır.

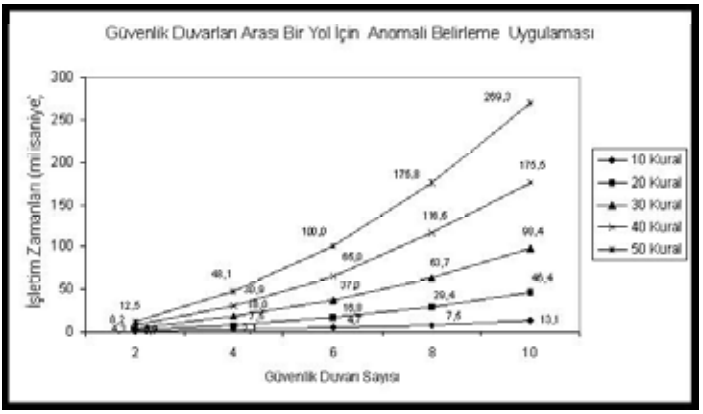
Politika Anomali Belirleyicisi, değişik kural sayıları için, yirmiden ikiyüze kadar yirmişer yirmişer, dört kural listesi üzerinde güvenlik duvarı içi anomalilerini belirlemek için çalıştırılmıştır. Her durum için işlem zamanları ölçülmüş ve sonuçlar Şekil 4'de gösterilmiştir. Elde edilen sonuçlar [4]'de verilen sonuçlar ile tutarlıdır.

Güvenlik duvarları arası anomali belirleme uygulamasının işletimsel değerleri-nin tespit edilmesi için iki farklı deney gerçekleştirilmiştir. İlk deneyde anomali belirleme uygulaması bir patika üzerinde olan bir grup güvenlik duvarı için işletilmiştir.

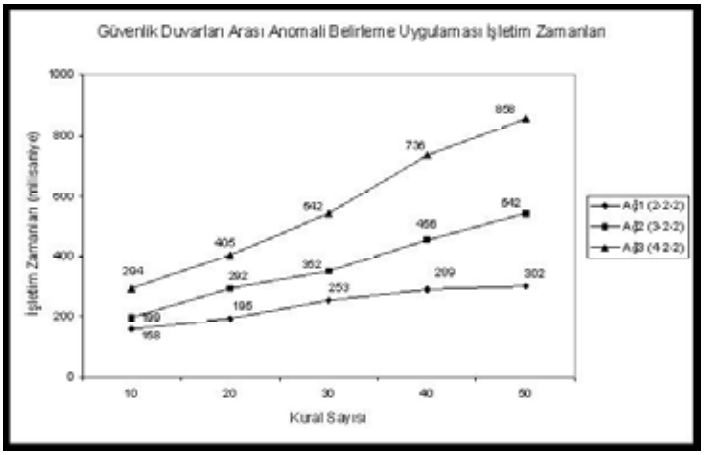
Şekil 4. Güvenlik Duvarı İçi Anomali Belirleme Uygulaması İşletim Zamanı



Şekil 4. Güvenlik Duvarı İçi Anomali Belirleme Uygulaması İşletim Zamanı



Şekil 5. Güvenlik Duvarları Arası Anomali Belirleme Uygulaması Bir Patika İçin İşletim Zamanı



Şekil 6. Güvenlik Duvarları Arası Anomali Belirleme Uygulaması İşletim Zamanı

Kullanılan kurallar bir önceki deneydeki iki numaralı kural listesi kurallarına benzemektedir. Her güvenlik duvarındaki kural sayıları ve yol üzerindeki güvenlik duvarları adetleri arttırılmıştır. Bu deneyin oluşturulma mantığı [4]'den alınmıştır. Sonuçlar Şekil 5'de gösterilmiştir. Elde edilen sonuçlar [4]'de verilen sonuçlar ile tutarlıdır.

Şekil 5'de gösterildiği gibi güvenlik duvarları arası anomali belirleme uygulaması-nın işlem zamanı güvenlik duvarı içi anomali belirleme uygulamasının işlem zamanına çok yakındır. Örneğin her birinde 40 kural bulunan iki güvenlik duvarı için işlem zamanı 8.2 milisaniyedir. Bu değer 80 kural içeren güvenlik duvarı içi anomali belirleme uygulamasının sonuç değerine neredeyse eşittir.

İkinci deneyde güvenlik duvarları arası anomali belirleme uygulaması farklı ağ topolojileri kullanılarak çalıştırılmıştır. Uygulamanın işletilmesi sırasında kullanıla-cak olan topolojiler üç farklı ağ için şöyle oluşturulmuştur: ağ1(2-2-2), ağ2(3-2-2), ağ3(4-2-2). Örneğin ağ2'de kök düğümün 3 dalı, seviye iki ve seviye üçte ise her bir düğümün 2 dalı mevcuttur. Ağda bulunan her bir güvenlik duvarı için rastgele kurallar tanımlanmıştır. Bu deneyin oluşturulma mantığı [4]'den alınmıştır. Her bir ağda, politika anomali sonucunun üretilmesi için gerekli olan işletim süresi ölçülmüş ve sonuçlar Şekil 6'da gösterilmiştir. Elde edilen sonuçlar [4]'de verilen sonuçlar ile tutarlıdır.

Elde edilen sonuçlarda güvenlik duvarları arası anomali belirleme uygulama-sının, altağlar arasındaki patikaların toplam sayısına bağlı olduğu görülmektedir. Zira ağ3'ün, ağ1 ve ağ2'ye göre daha fazla sayıda patikası vardır ve ağ3 için uygulamanın işletim zamanı diğerlerinden daha fazladır.

5. Laboratuvar Deneyleri

Güvenlik duvarları arası anomali belirleme uygulamasının işletim değerlerinin gerçek bir dağıtık ortamda, diğer bir deyişle laboratuvar ortamında, tespit edilmesi için deneyler yapılmıştır. Deney ortamı Şekil 7'de gösterildiği gibidir.

İnternet'ten istemciye doğru olan trafik akışı gd1-gd2-gd3-gd4-gd5 üzerinden-dir ve istemciden İnternet'e trafik akışı gd5-gd4-gd3-gd2-gd1 üzerindendir. Bütün güven-lik duvarları iki adet 10/100Mbs PCI Ethernet kart ağ arabirimlidir ve 48 port Cisco anahtarlayıcısına bağlıdırlar. Politika Anomali Belirleyicisi, Pentium IV-M 1.73 GHz. ve 1.49 GByte RAM olan bir bilgisayar üzerinde kuruludur. Güvenlik Duvarı Etmeni ile iletişimi için soket programlama işlevselliği eklenmiştir. Phyton programlama dili kullanılarak geliştirilen Güvenlik Duvarı Etmeni yol üzerindeki her bir güvenlik duvarı üzerinde kuruludur. Temel işlevi güvenlik duvarının Politika Anomali Belirleyicisi ile iletişimini sağlamaktır. Politika Anomali Belirleyicisi ile Güvenlik Duvarı Etmeni arasındaki iletişimin dört adımı vardır:

Adım1: Güvenlik Duvarı Etmeni Politika Anomali Belirleyicisine politikasına ekleyeceği yeni kuralı gönderir.

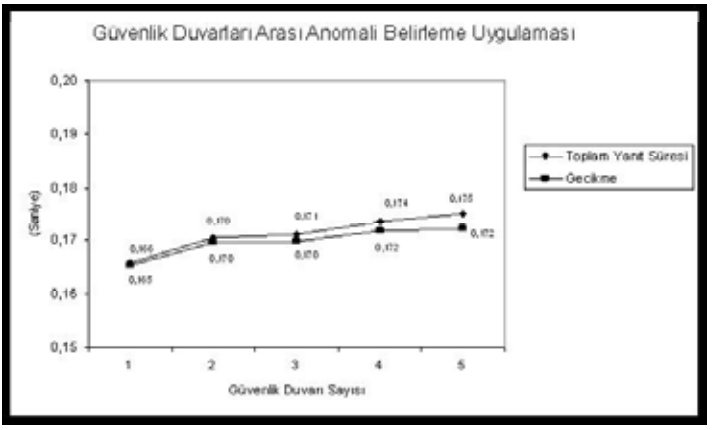
Adım2: Politika Anomali Belirleyicisi kuralı alır, diğer kurallarla ilişkilerini kontrol eder ve anomali sonucunu Güvenlik Duvarı Etmenine bildirir.

Adım3: Eğer anomali tespit edilmemiş ise, Güvenlik Duvarı Etmeni yeni kuralı politikasına ekler ve değişen politikayı Politika Anomali Belirleyicisine gönderir. Anomali var ise ekleme yapılmaz.

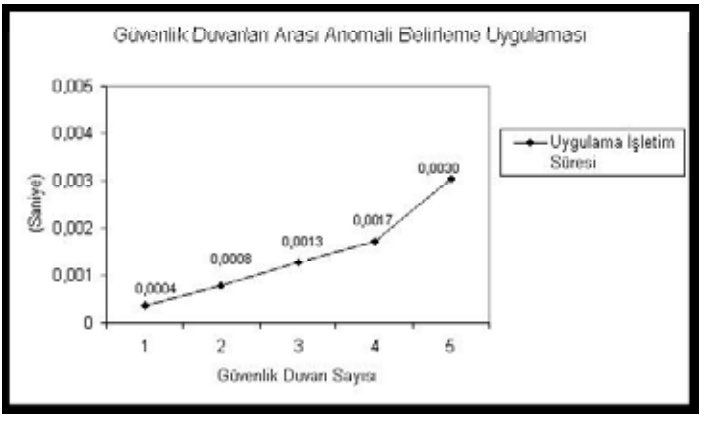
Adım4: Güvenlik Duvarı Etmeni "anomali var" veya "anomali yok" uyarı mesajını görüntüler.

İlk olarak Güvenlik Duvarı Etmeni tarafından yeni kural gd1'den Politika Anomali Belirleyicisine gönderilir. Yeni kural alındığında o güvenlik duvarına ait politikaya eklenir ve güvenlik duvarları arası anomali belirleme uygulaması işletilir. Uygulamanın sonunda anomali sonuçları Güvenlik Duvarı Etmenine gönderilir.

Bu deney patika üzerindeki her bir güvenlik duvarı için tekrarlanır. Her güvenlik duvarı için toplam yanıt zamanı ve güvenlik duvarları arası anomali bulma uygulaması işletim süresi ölçülmüştür. Toplam yanıt zamanı Güvenlik Duvarı Etmeni tarafından ve güvenlik duvarları arası anomali bulma uygulaması işletim süresi Politika Anomali Belirleyicisi tarafından ölçülmüştür ve gecikme süresi (toplam yanıt zamanı - güvenlik duvarları arası anomali bulma algoritması işletim süresi) formulünden hesaplanmıştır. Sonuçlar Şekil 8 ve Şekil 9'da gösterilmiştir.



Şekil 8. Güvenlik Duvarları Arası Anomali Belirleme Uygulaması Deneyi İçin Toplam Yanıt ve Gecikme Süreleri



Şekil 9. Güvenlik Duvarları Arası Anomali Belirleme Uygulaması Deneyi için İşletim Süreleri

Bu sonuçlar güvenlik duvarları arası anomali belirleme uygulaması işletim sürelerinin Şekil 5'de bulunan güvenlik duvarları arası anomali belirleme uygulaması işletim sürelerine çok yakın olduğunu göstermektedir.

6. Sonuç

Bu çalışmada tek ve dağıtık güvenlik duvarı ortamları için politika anomali belirleme algoritmaları "Politika Anomali Belirleyicisi" adı verilen bir yazılım aracında uygulanmıştır. Güvenlik duvarlarının doğru çalışması filtreleme kurallarına ve bu kuralların sıralamasına bağlıdır. Eğer aynı paket, politika içindeki birden fazla filtreleme kuralına uyuyor ise güvenlik duvarı içi politika anomalisi olabilir. Eğer bir ağ patikası üzerindeki iki güvenlik duvarı aynı trafik üzerinde farklı eylemler gösteriyor ise güvenlik duvarları arası politika anomalisi olabilir. Doğru kural sıralamasının belirlenmesi için kurallar arasındaki matematiksel ilişkiler dikkate alınmalıdır.

Literatürde matematiksel zemin ve ilgili algoritmalar mevcuttur. Algoritmaların [4]'de uygulanmış ve bazı deneysel sonuçların verilmiş olmasına rağmen uygulama detayları açık değildir. Politika Anomali Belirleyicisi, Java programlama dili ile nesneye dayalı tasarım metodları kullanılarak geliştirilmiştir. Anılan literatürde yapılmış olan deneyler aynı ve değişik parametreler ile tekrarlanmış ve literatürde verilen sonuçlarla tutarlı değerler elde edildiği gözlenmiştir. Gerçek bir dağıtık güvenlik duvarı laboratuvar ortamında konuşlandırılmış ve bu konfigürasyon üzerinde çalışma deneyleri tekrarlanmıştır. Anılan konfigürasyon ve bu konfigürasyon üzerinde yapılan deneyler ile sonuçları literatürde mevcut değildir.

Politika Anomali Belirleyicisi güvenlik duvarı içi ve güvenlik duvarları arası anomalileri belirler. Politika yönetimi için kural ekleme ve kural çıkartma işlevselliği eklenebilir. Aynı alandaki diğer anomali belirleme algoritmaları uygulanarak bu çalışmanın sonuçları ile karşılaştırılabilir. Politika Anomali Belirleyicisi kullanılabilir-liğinin belirlenmesi amacıyla daha geniş ve yaşayan ortamlarda, kampüs ortamı gibi, deneyler gerçekleştirilebilir.

7. Kaynaklar

[1]. Chapman, B., and Zwicky, E., *Building Internet Firewalls*, O'Reilly, 1995.

[2]. Wack, J., Cutler, K. and Pole, J., *Guidelines on Firewalls and Firewall Policy*, NIST Special Publication, No: 800-41, 2002.

[3]. Al-Shaer, E.S. and Hamed, H.H., "Discovery of Policy Anomalies in Distributed Firewalls", 23rd Annual Joint Conference of the IEEE Computer and Communications Societies, March 2004, Hong Kong, China.

[4]. Al-Shaer, E.S., Hamed, H.H., Boutaba, R. and Masum, H., "Conflict Classification and Analysis of Distributed Firewall Policies", *IEEE Journal on Selected Areas in Communications*, Oct. 2005, Volume: 23, Issue: 10, 2069-2084.