Mobil Tasarsız Ağlarda Saldırı Tespiti

Sevil Şen[1] John A. Clark[2]

[1,2]Department of Computer Science, University of York, York, UK
[1]e-posta: ssen@cs.york.ac.uk [2] e-posta: jac@cs.york.ac.uk

Özetçe

In recent years mobile ad hoc networks (MANETs) have become very attractive for many applications such as tactical and disaster recovery operations. However they are more vulnerable to attacks than wired networks. In addition, conventional intrusion detection systems (IDS) are ineffective and inefficient for this new environment. IDS design on MANETs is a complex engineering task due to their very nature. The presence of complication factors such as highly constrained nodes requires complex tradeoff to be made. In this paper we show how Genetic Programming together with a Multi-Objective Evolutionary Algorithm (MOEA) can be used to synthesise intrusion detection programs that make optimal trade-offs between security criteria and the power they consume.

1. Giriş

Mobil tasarsız ağlar kendinden yapılı, mobil düğümler ile telsiz bağlantıların bir araya gelmesi ile oluşan ağlardır. Bu ağlar önceden kurulmuş, sabit bir yapıya sahip değillerdir. Bu özellikleri, onları, birçok uygulama için çekici kılmıştır. Askeri uygulamalar, sabit yapının kurulmasının olanaksız olduğu afet (sel, deprem, vb.) kurtarma operasyonları ilk akla gelen örneklerdir. Ama bu ağlar doğaları gereği saldırılara karşı daha dayanıksızdırlar. Sağlam bir güvenlik sisteminin gereği olarak bu saldırıları engelleyebilmeli, engelleyemediğimiz durumlarda tespit edebilmeliyiz. Güvenlik sisteminin vazgeçilmez bir parçası olan saldırı tespit sistemleri (STS), ağı izleyerek saldırıları tespit eder ve bu saldırılara cevap verir.

Literatürde kablolu ağlar için önerilmiş bir çok saldırı tespit sistemi vardır. Ama mobil tasarısız ağların onlara has özellikleri -mobilite, kısıtlı kaynaklara sahip düğümler, merkezi yönetim düğümlerinin eksikliği- bu sistemlerin bu ağlara direk uygulanmasını olanaksız kılmıştır. Bu nedenle araştırmacılar, bu ağlar için yeni saldırı tespit sistemleri geliştirmek veya varolan sistemleri bu ağlara adapte edebilmek üzerine yoğunlaşmışlardır. Biz de bu çalışmamızda, bu karmaşık özellikli ağlar için evrimsel hesaplama yöntemlerinden yararlanarak bir saldırı tespit sistemi önerdik. Bu yöntem ile bu ağlar üzerinde bilinen saldırıları tespit etmek için evrim teorisinden faydalanarak programlar geliştirdik. Bu programların bilinen saldırıları başarı ile tespit ettiğini değişik simülasyonlarda (farklı trafik ve mobilite seviyelerine sahip ağlarda) gösterdik. Dahası, çoklu optimizasyon evrimsel hesaplama yöntemlerini uygulayarak, güç kaynağı kısıtlı bu ağlar üzerinde hem etkili hem de daha az enerji harcayan programların evrimleştirilmesi araştırdık.

2. Yapılan Çalışmalar

Evrimsel hesaplama yöntemlerini kullanarak saldırı tespit sistemi evrimleştirmeyi amaçlayan çalışmalar genellikle genetik programlama (GP) ya da genetik algoritmaları (GA) kullanmışlardır. Yakın zamanda GP kullanarak kablolu ağlar için STS geliştiren bir çalışma [10]'da önerilmiştir. Bu çalışmadaki temel fikir, verilen özellikleri ve işleçleri kullanarak otomatik bir saldırı tespit programı geliştirmektir. Çıktı programı küçük ve basittir. Saldırı tespiti için birçok makine öğrenme yöntemi tüm özellikleri kullanırken, önerilen çalışmada GP, az sayıda özellik kullanmıştır [10]. Bu çalışmada GP yöntemleri diğer bazı yöntemler (SVM, Karar ağaçları) ile karşılaştırılmıştır ve daha iyi performans sergilediği gösterilmiştir. Genetik algoritma yönteminin kablolu ağlar için saldırı tespit sistemleri üzerinde de ümit verici uygulamaları bulunmaktadır [12][13]. Diğer bir evrimsel hesaplama yöntemi olan gramatiksel evrimleşme, kablolu ve mobil tasarsız ağlarda saldırı tespiti için yakın zamanda önerilmiştir [14][15].

Mobil tasarısız ağlarda saldırı tespiti için son on senedir çalışmalar yapılmaktadır. En çok kullanılan yöntem, spefikasyona bağlı tespit etme yöntemidir [19]. Bu yöntemde, rota tespit etme protokollerinin spesifikasyonları tanımlanır ve bu spesifikasyonlara uymayan durumlar saldırı olarak tespit edilir. Yapay zeka yöntemlerini uygulayarak ağdaki normal olmayan durumları tespit eden yöntemler de önerilmiştir [8][16]. Az sayıda da olsa saldırı imzası ile saldırıları tespit eden yaklaşımlar da literatürde bulunmaktadır [18]. Mobil tasarısız ağlar için önerilmiş saldırı tespit sistemlerinin güncel, daha ayrıntılı incelemesi için okuyucu [17] çalışmaya başvurabilir.

3. Mobil Tasarsız Ağlarda Saldırı Tespiti

Bu çalışmanın temel amacı, mobil tasarsız ağlar üzerindeki bilinen saldırıların etkili ve verimli bir şekilde tespit edilmesidir. Bu çalışmada ele alınan saldırılar aşağıda açıklanmıştır. Deneylerimizde, mobil tasarısız ağlar için geliştirilmiş en çok kullanılan rota tespit etme protokollerinden biri olan AODV [1] kullanılmıştır.

Rota İstemi Taşkın Saldırıları: Mobil tasarsız ağlarda ağ topolojisi, ağdaki düğümlerin mobilitesine bağlı olarak sık olarak değişmektedir. Dahası, bağlantı kopuklukları telsiz ağlarda pek yaygındır. Bu durumlar varolan bağlantıların bozulmasına ve rota arama (RREQ) paketleri ile yeni bağlantıların aranmasına neden olur. Bu paketler, AODV gibi tepkisel rota tespit etme protokolleri tarafından, düğümler

yeni bir rotaya ihtiyaç duyulduğunda gönderilir. Mobilitenin ağdaki RREQ paketlerinin sayısını arttırabileceği açıkça görülmektedir. Rota istemi taşkın saldırısında saldırgan, bu rota tespit etme mekanizmasını istismar eder ve rastgele hedef düğümler için ağa birçok RREQ paketi yayımlar. Saldırganın amacı düğümlerin ve ağın kaynaklarını tüketmektir. Ning ve Sun [7]'un çalışmasında olduğu gibi simülasyonumuzda saldırgan, amacını gerçekleştirmek için birim zamanda ard arda 20 RREQ paket göndermektedir.

Rota Bozma Saldırıları: Bu saldırıda, saldırgan kurbanına rota istemi (RREQ) paketi almadan rota cevabı (RREP) paketleri gönderir. Rastgele düğümlere RREQ paketi göndermektense, saldırgan komşularından birini kurban olarak seçer ve bu düğümün rota tablosunu bozmak için ona yeni (daha büyük düğüm sıra numarası ile) RREP paketleri gönderir. Saldırgan, kurbanın komşusu olduğu ve kurban tarafından yayınlanan paketleri duyduğu için bu düğümün aktif rotalarını bilmektedir. Sun'un çalışmasında [8] belirtildiği gibi sadece birkaç yanlış rota tespit etme paketi ile saldırgan ağa zarar veremez. Bu nedenle simülasyonumuzda saldırgan, kurbana birim zamanda 5-10 RREP paket göndermektedir.

4. Saldırı Tespiti için Evrimsel Hesaplama Yöntemlerinin Uygulanışı

Evrimsel hesaplama yöntemleri, bilgisayar programlarının otomatik olarak yaratılması için bir çatı sağlar. Bu yöntemler, öncelikle bireylerden oluşan bir populasyon yaratırlar, bu bireyler hedef problemin çözümü için üretilen adaylardır. Daha sonra populasyondaki her bir birey değerlendirilir ve birer uygunluk değeri verilir. Bu uygunluk değeri bir bireyin, hedef problemi ne kadar iyi çözdüğünü ya da çözmeye ne kadar yaklaştığını gösterir. Bitirme kriteri sağlanana kadar, seçim, mutasyon, eşleşme gibi doğal evrim işleçleri kullanılarak yeni populasyonlar üretilir. Bu genetik işleçler, yeni populasyonlarda daha iyi bireylerin üretilmesini sağlamak için kullanılır. Seçim işleçi, daha iyi (çözüme yakın) bireylerin hayatta kalmasını sağlar. Eşleşme, bireyler arasındaki DNA değişimini taklit eder. Mutasyon ise doğal mutasyonun bir yansımasıdır ve çeşitliliği sağlar.

4.1. Genetik Programlama

Bu çalışmamızda, yukarıda tanımlanan rota istemi taşkın saldırıları ve rota bozma saldırılarını tespit edebilmek için, literatürde en çok uygulanan evrimsel hesaplama yöntemlerinden biri olan Genetik Programlama(GP)'yı kullandık. Her bir saldırıyı tespit etmek için programları evrimleştirdik ve bu programları farklı ağlar (farklı mobilite ve farklı trafik seviyelerinde) üzerinde test ettik.

GP'de bir problem fonksiyonlar, özellikler ve uygunluk değeri ile tanımlanır ve her bir birey ağaç yapısı ile gösterilir. Bu çalışmada kullanılan özellikler Ek A'da verilmiştir. Mobilite ve ağdaki paketler hakkında bilgi veren bu özellikler, ağdaki düğümler tarafından her birim zamanda toplanılır. Bazı özellikler, örneğin komşu düğümlerdeki değişimler, mobilite hakkında direkt bilgi verirler. Bazıları ise, örneğin son zaman aralığında eklenen rotaların sayısı, ağdaki mobilitenin bir sonucudur. Ağdaki paketler ile ilgili özellikler, birim zamanda bir düğüm tarafından alınan, gönderilen rota tespit etme protokolü paketlerinin sayısı hakkında bilgi verir. Bu çalışmada kullanılan fonksiyonlar ile GP parametreleri Tablo 1'de sunulmuştur.

Populasyon büyüklüğü herhangi bir nesildeki bireylerin sayısını tanımlar. *Yineleme sayısı* evrimin ne zaman, hangi nesilde biteceğini gösterir. *Eşleşme olasılığı* seçilen bireylerin hangi olasılıkla eşleştirileceğini (eşleştirme işlecinin uygulanacağını) tanımlar. *Kopyalama olasılığı* hangi olasılıkla bireyin, hiçbir değişime uğramadan bir sonraki populasyona aktarılacağını gösterir. Turnuva seçimi, eşleştirme amaçlı bireylerin seçiminde kullanılan yöntemlerden birisidir. Bu yöntemde, öncelikle bir grup birey varolan populasyondan rastgele olarak seçilir, daha sonra bu gruptaki en iyi (uygunluk değeri en yüksek) birey eşleştirme amaçlı seçilir. *Turnuva büyüklüğü* bu grupun büyüklüğünü belirtir. GP gerçekleştirimi için ECJ 18 [4] kullanılmıştır. Tablo 1'de listelenmeyen parametreler, ECJ 18'nin varsayılan parametreleridir.

Tablo 1: GP Parametreleri

Amaç	Rota istemi taşkın ve rota bozma saldırılarını tespit eden programların bulunması
Fonksiyon Kümesi	+, -, *, /, min, mak, yüzde, log, ln, sin, cos, kare kök, mutlak değer, üs, ve, veya, karşılaştırma işleçleri
Özellikler	Ek A'da verilmiştir.
Populasyon Büyüklüğü	100
Yineleme Sayısı	1000
Eşleşme Olasılığı	0.9
Kopyalama Olasılığı	0.1
Turnuva Büyüklüğü	7

Uygunluk değeri, bir bireyin (çözüm için üretilen adayın) değerini ölçtüğü için çok önemlidir. Deneylerimizde kullanılan uygunluk değeri aşağıda tanımlanmıştır. Tespit oranı (TO), doğru olarak tespit edilen saldırılan, simülasyondaki tüm saldırılara oranıdır. Yanlış tespit oranı (YTO), saldırı olmayıp evrimleştirilmiş programlar tarafından saldırı olarak tespit edilen durumların, simülasyondaki normal durumlara (saldırının olmadığı) oranıdır. Yanlış tespit oranının küçük olması, tespit oranının büyük olması kadar önemlidir. Çok sayıda yanlış tespit oranı, zaman kaybına neden olur ve STS'nin güvenilirliğini azaltır.

$$\textit{Uygunluk değeri} = \textit{tespit oranı} - \textit{yanlış tespit oranı} \quad (1)$$

4.2. Sonuçlar

Deneylerimizde, ağ simülasyonları için ns-2 [2] kullandık. Mobilite örüntüleri ise BonnMotion[3] ile oluşturulmuştur. Farklı mobilite ve trafik seviyelerinde farklı ağ senaryoları oluşturduk. Simülasyon parametreleri Tablo 2'de verilmiştir.

Saldırı tespit programlarını eğitmek için, orta seviyede mobilite ve trafik seviyesine sahip bir ağ kullanılmıştır. Yanlış tespit oranını azaltmak için, sistemi eğitirken aynı ağın hem saldırı altında hem de saldırısız durumdaki simülasyonları beraber kullanılmıştır. GP algoritması her saldırı için on kez çalıştırılmış ve en iyi birey seçilmiştir.

Tablo 2: Ağ Simülasyonu Parametreleri

Ağ Boyutları	1000x500
Düğüm Sayısı	50
Paket Trafiği	20 ve 30 TCP bağlantısı
Hız	0-20 m/sn
Durma Süresi	40, 20, 5 sn. (düşük, orta, yüksek mobilite)
Rota Tespiti Etme Protokolü	AODV
Lokal Bağlantıların Kontrolü	AODV periyodik Hello paketleri
Simülasyon Süresi	2000 sn. (öğrenme), 1000 sn. (test)

Her saldırı için ayrı bir program evrimleştirilmiştir. Evrimleşmiş programlar ağdaki her bir düğüme dağıtılmıştır. Saldırıların, etkilediği düğümler tarafından tespit edileceği varsayılmıştır. Rota istemi taşkın saldırıları, RREQ paketlerinin taşkınına uğramış düğümler tarafından tespit edilecektir. Rota bozma saldırıları ise yanlış RREP paketlerine maruz kalan kurban düğüm tarafından tespit edilecektir. Tablo 3'te her bir saldırı için evrimleştirilmiş en iyi programın (bireyin) performansı görülmektedir.

Tablo 3: Evrimleştirilmiş Programların Performansı

Ağ Simülasyonu	**Rota İstemi Taşkın Saldırıları**		**Rota Bozma Saldırıları**	
	TO	**YTO**	**TO**	**YTO**
düşük mobilite düşük trafik	%99.81	%0.34	%100	%0.51
düşük mobilite orta trafik	%99.24	%1.94	%100	%0.99
orta mobilite düşük trafik	%99.95	%0.36	%97.06	%0.46
orta mobilite orta trafik	%99.89	%1.88	%100	%0.88
yüksek mobilite düşük trafik	%99.79	%0.66	%100	%0.52
yüksek mobilite orta trafik	%98.62	%1.83	%100	%0.84

Deney sonuçları, rota bozma saldırılarının, rota istemi taşkın saldırılarından daha kolay tespit edilebileceğini göstermiştir. Rota bozma saldırıları için bir durum hariç her durumda, maksimum tespit oranı (%100) sağlanmıştır ve yanlış tespit oranı %1'den düşüktür. En iyi tespit oranı orta mobilite ve düşük trafik düzeyindeki ağda sağlanamamıştır, ama bu durumda FTO oranı düşüktür. En iyi tespit oranının FTO'da azıcık bir yükselme ile elde edilebileceğini varsaymak makuldur. Rota istemi taşkın saldırılarında ise TO oranı her zaman %99 üzerinde iken FTO oranı da kabul edilebilir bir ölçüde düşüktür. Her iki saldırıda da, asıl problemin mobilite örüntüsünden farklı olarak yüksek trafikten kaynaklandığı gözlenmiştir. Orta seviyede trafikte FTO oranı, her zaman düşük seviye trafikte olduğundan daha fazladır. Bu durum, mükemmel sonucu bulamayan her saldırı tespit sisteminin yaşadığı bir durumdur. Daha çok trafik analiz edildiğinde, dolaylı olarak yanlış tespit oranı da artar.

5. Enerji Farkında Saldırı Tespiti

Mobil tasarısız ağlardaki düğümler cep telefonlarından, diz üstü bilgisayarlarına kadar çok çeşitli olabilir. Bu cihazlar, farklı kaynak ve işleme kapasitesine sahiptirler. Dahası, bu cihazlar mobiliteyi sağlamak amacı ile genellikle pil gücü ile çalışır. Değişik çeşitlerdeki düğümler, özellikle kısıtlı kaynaklara sahip, saldırı tespit sisteminin de doğru çalışmasını etkiler. Örneğin, saldırı tespit sistemleri kısıtlı kaynaklar nedeni ile gelen her paketi işleyemeyebilirler. Bu nedenle, mobil tasarısız ağlarda bir saldırı tespit sisteminin verimliliği, etkinliği kadar önem kazanır.

Bu çalışmada, saldırı tespit programlarını çalıştıran düğümlerin de kapasitelerini de ele alarak bu programların evrimleştirilmesini araştırdık. Çoklu optimizasyon tekniklerini kullanarak bir programın fonksiyonel ve fonksiyonel olmayan özellikleri arasındaki takası inceledik. Güç, mobil tasarısız ağlarda en önemli kaynaklardan biri olduğu için, programları evrimleştirirken tespit oranı yanında harcadıkları enerjiyi de birer uygunluk değeri olarak göz önüne aldık.

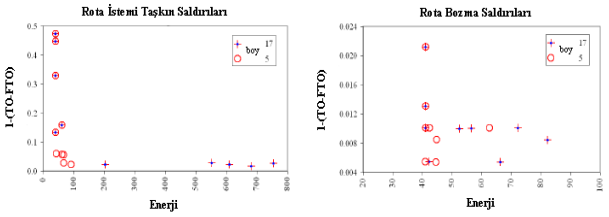
5.1. Evrimleştirilen Programların Güç Harcamasının Analizi

Öncelikle, rota istemi taşkın ve rota bozma saldırılarını tespit etmek için GP ile evrimleştirilmiş programların güç harcamalarını inceledik. Bir programın enerji harcamasını hesaplayabilmek için öncelikle o programın çalışmasını simüle etmemiz gerekmektedir. Bu amaçla, GP ağaçlarını C programına çevirip, bir kütüğe kaydettik. C kütüğü oluşturulduktan sonra, Sim-Wattch simülatoru kullanılarak programın PISA mimarisi üzerindeki çalışması simüle edilmiş ve enerji harcaması hesaplanmıştır. Wattch [9], mikro işlemcilerin güç harcamalarını inceleyen ve optimize eden bir çatıdır. Sim-Wattch, Wattch'ın güç modellerini SimpleScalar [5] mimari simülatorü ile birleştirmiştir.

Şekil 1'de, 4. Bölümde evrimleştirilmiş on programın performansları (uygunluk değerleri) ve enerji harcamaları verilmiştir. Bu şekilde, rota istemi taşkın saldırılarını tespit etmek için evrimleştirilmiş bir programın sınıflandırma doğruluğu (TO – YTO) arttığında, o programın enerji harcaması da artmıştır. Ama bu ilişki rota bozma saldırıları için o kadar açık değildir. Bu saldırı için evrimleştirilmiş programları incelediğimizde, bu saldırının basit bir saldırı olduğu ve küçük bir program (genellikle az enerji harcayan) ile tespit edilebileceğini farkettik.

Bir programın büyüklüğü, o programın enerji harcamasını etkileyebilir. Bu nedenle, deneylerimizi farklı ağaç boylarında (5, 17) da uygulayarak geliştirdik. Ağaç boyu, GP'de evrimleştirilmiş bir ağacın boyunu tanımlar. Şekil 2'de ağaç boyunun evrimleştirilmiş programların tespit edebilme yetenekleri ve enerji harcamaları üzerindeki etkileri görülmektedir. Daha önce belirtildiği gibi rota bozma saldırıları küçük programlar ile tespit edilebilir. Ama ağaç boyu, daha küçük programların, dolayısı ile daha az enerji

harcayan programların evrimleştirilmesini sağlamıştır. Bu nedenle, Şekil 1'de bu saldırıyı tespit etmek için diğer ağaç boyunda evrimleştirilmiş programlar ile aynı performansı gösteren fakat daha az enerji harcayan programları da görmekteyiz. Rota istemi taşkın saldırıları için sonuçlar daha çarpıcıdır. Sonuçlarda, bu saldırının küçük programlar ile de başarı ile tespit edilebileceği görülmektedir. Ama daha büyük, dolayısıyla daha fazla enerji harcayan programların, bu saldırıyı tespit etmede daha iyi bir performans sergilediği gözlenmiştir.



Şekil 1: Evrimleştirilmiş programların enerji harcalamarı ve sınıflandırma doğrulukları.

Bu deneyler, bu iki hedef (programın saldırıları etkin bir şekilde tespit etmesi ve az enerji harcaması) arasındaki takas ilişkilerini bulmamız için bizi teşvik etmiştir. Bu ilişkileri keşfedebilmek için bir sonraki bölümde açıklanan çoklu amaç evrimsel hesaplama tekniklerini kullandık.

5.2. Çoklu Amaç Evrimsel Hesaplama (ÇAEH)

Çoklu amaç optimizasyonu iki veya daha fazla amacı, genellikle birbiri ile çelişen, aynı anda optimize etmeye çalışır. Genellikle çoklu amaç optimizasyou tek bir çözüm önermez, optimal çözümlerin yer aldığı bir küme önerir. Bu kümeye Pareto kümesi denir. Bu yaklaşımda, eğer bir x vektörünün bileşenlerinden hiçbiri bir y vektörünün bileşenlerinden büyük değil ve en az bir bileşeni küçük ise (küçük değerler tercih edilir), x y'ye baskındır (x ϕ y) denir.

$$x \phi y : \text{tüm i'ler için } x_i \leq y_i \text{ ve en az bir j için } x_j < y_j \text{ ise} \quad (2)$$

Pareto eğrisi, başka bireyler tarafından üzerinde baskınlık kurulmamış bireyleri içerir. Diğer bir deyişle, amaçlar arasındaki takasları gösteren optimal çözümleri içerir.

Çoklu amaç evrimsel hesaplama (ÇAEH), bize çoklu amaç optimizasyon teknikleri ile evrimsel hesaplama yöntemlerini birleştirme imkanı verir. Deneylerimizde popüler ÇAEH algoritmalarından biri olan SPEA2 algoritması [6] kullanılmıştır.

5.3. Enerji Farkında Saldırı Tespit Programların Evrimleştirilmesi

Çoklu amaç evrimsel hesaplama yöntemlerini kullanarak, şu üç amacı optimize etmeyi hedefledik : tespit oranı, yanlış tespit oranı, ve programların enerji harcaması. Birey, bu üç amaç üzerindeki performansına bağlı olarak evrim sürecinde yer alır. Bir bireyin çoklu amaç fonksiyonu aşağıda verilmiştir. Bu üç amacın aynı anda maksimize edilmesi hedeflenmiştir.

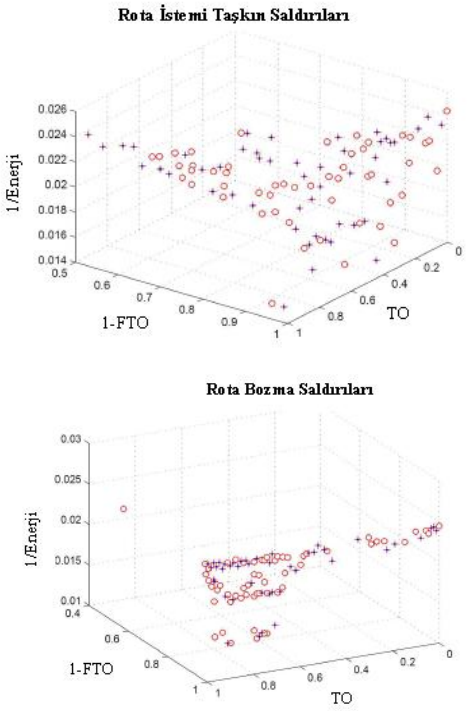
f_1 = başarı ile tespit edilen saldırılar / tüm saldırılar (3)

f_2 =1 – saldırı olarak tespit edilen normal durumlar / tüm normal durumlar (4)

f_3 = 1 / enerji harcaması (5)

Öncelikle, rota istemi taşkın ve rota bozma saldırıları için ÇAEH yöntemlerini kullanarak ayrı ayrı programlar evrimleştirdik. Populasyon büyüklüğü (150) ve SPEA2 arşiv büyüklüğü dışında (100) Tablo 1'deki parametreler kullanılmıştır. Şekil 2, 1000. yinelemede bulunan optimal çözümleri göstermektedir (yuvarlaklar pareto eğrisini göstermektedir). Rota istemi taşkın saldırılarında Pareto eğrisi, TO büyük ve FTO düşük bireyler için yüksek enerji harcamasına doğru kayar. Sonuçlar açıkça göstermiştir ki FTO, enerji harcamasından etkilenmektedir. FTO'da artış, enerji harcamasında azalmaya neden olmaktadır.

Rota bozma saldırıları için optimal çözüme yakın programlar elde edilmiştir. ÇAEH yöntemi ile evrimleştirilmiş programları, sadece GP yöntemi kullanılarak evrimleştirilen programlar ile karşılaştırdık ve ÇAEH ile daha az enerji harcayan programları bulabildiğimizi gördük. Özellikle rota istemi taşkın saldırıları için enerji harcaması, bu yöntem ile önemli ölçüde düşmüştür.



Şekil 2: Saldırıların tespiti için evrimleştirilmiş programların 3 Boyutlu Pareto eğrisi.

Son olarak, ÇAEH yöntemi ile rota istemi taşkın ve rota bozma saldırılarını beraber tespit eden programlar evrimleştirdik. Bu deney ile şu soruya cevap aradık : "enerji harcaması açısından her saldırı için ayrı bir program mı, yoksa iki program için tek bir program mı geliştirmek daha iyidir ?". Bu deneyin sonuçları göstermiştir ki iki saldırıyı tek bir program ile, iki ayrı saldırı tespit programının

yapabilceğinden daha enerji verimli bir şekilde tespit edebiliriz. Ama bu programların TO (%94 <) ve FTO (> %6) oranlarına bakıldığında, hiçbir program diğer iki program kadar yüksek performans gösterememiştir. Kullanıcı, mobil tasarısız ağ uygulamasının gereksinimlerine göre bu amaçlar arasında takas yapabilir.

6. Sonuç

Bu çalışmada, bilinen rota istemi taşkın ve rota bozma saldırılarını tespit eden programlar GP yöntemi ile evrimleştirilmiş ve değişik mobilite ve trafik seviyelerine sahip ağlar üzerinde test edilmiştir. Bu programların saldırıları tespit etmede iyi bir performans gösterdiği sergilenmiştir. Ama kısıtlı kaynaklara sahip bu ağlar için saldırı tespit sisteminin verimliliği de çok önemlidir. Bu çalışmadaki deneylerde hem tekli hem de programların enerji harcamasını da ele alan çoklu amaç uygunluk değerleri kullanılmıştır. Bazı durumlarda çoklu amaç optimizasyon yöntemleri ile takas uzayının daha etkili bir şekilde araştırılabilceği gösterilmiştir. Bu çalışma, saldırı tespit programların etkinliği ve verimliliği arasında takas yapması açısından yeni bir yaklaşımdır. Bu yaklaşım kısıtlı kaynaklara sahip bazı ağlar için (mobil tasarısız ağlar, algılayıcı ağlar) çok önemlidir ve biz araştırmacıları bu konuda çalışmaya davet ediyoruz.

7. Ek A: Özellikler

Özellikler (bir düğüm için)
komşu sayısı
birim zamanda eklenen komşu sayısı
birim zamanda silinen komşu sayısı
aktif rotaların sayısı
onarım halindeki rotaların sayısı
geçersiz kılınmış rotaların sayısı
rota keşif mekanizması tarafından eklenen rotaların sayısı
tesadüfen işitilen rotaların sayısı
değiştirilmiş rotaların sayısı (hop sayısı, sıra numarası değişimi)
onarılmak için eklenen rotaların sayısı
zaman aşımına uğradığı için geçersiz kılınmış rotaların sayısı
diğer nedenlerle geçersiz kılınmış rotaların sayısı
aktif rotaların ortalama hop sayısı
alınan RREQ paketlerinin sayısı
iletmek amacı ile alınmış RREQ paketlerinin sayısı
yayımlanan RREQ paketlerinin sayısı
iletilen RREQ paketlerinin sayısı
alınan RREP paketlerinin sayısı
iletmek amacı ile alınmış RREP paketlerinin sayısı
başlatılan (gönderilen) RREP paketlerinin sayısı
iletilen RREP paketlerinin sayısı
alınan RERR (rota hatası) paketlerinin sayısı (iletilecek olan ya da olmayan)
yayımlanan RERR paketlerinin sayısı
alınan rota tespit etme protokolü (AODV) kontrol paketlerinin sayısı
iletmek amacı ile alınmış AODV kontrol paketlerinin sayısı
gönderilen AODV kontrol paketlerinin sayısı
iletilen AODV kontrol paketlerinin sayısı

8. Kaynakça

[1] Perkins, C.E., Royer, E.M. "Ad-hoc on-demand Distance vector routing", *IEEE Workshop on Mobile Computer Ststems*, pp. 90-100. 1999.

[2] "Ns-2: The network simulator", http://www.isi.edu/nsnam/ns.

[3] "Bonnmotion: A mobility scenario generation and analysis tool", http://web.informatik.uni-bonn.de/IV/Mitarbeiter/dewaal/BonnMotion/.

[4] "ecj18: A java-based evolutionary computation research system", http://cs.gmu.edu/eclab/projects/ecj/.

[5] "Simplescalar", http://www.simplescalar.com/.

[6] Zitzler, E., Laumans, M., Thiele, L., "Spea2: Improving the strength pareto evolutionary algorithm", *Techinal Report 103, Swiss Federal Institute of Technology*

[7] Ning, P., Sun, K., "How to misuse AODV: A case study of insider attacks against mobile ad-hoc routing protocols", *IEEE Workshop on Information Assurance*, pp. 60-67, 2003

[8] Sun, B., Wu, K., Pooch, U.W., "Zone-based intrusion detection for mobile ad hoc networks", *Int. Journal of Ad Hoc and Sensor Wireless Networks*, 2(3), 2003

[9] Brooks, D., Tiwari, V., Martonosi, M., "Wattch: A framework for architectural-level power analysis and optimizations", *Int. Symposiyum on Computer Architecture*, 2000

[10] Abraham, A., Grosan, C., Martiv-Vide, C., "Evolutionary design of intrusion detection programs", *Int. Journal of Network Security*, 4:328-339, 2007

[11] Abraham, A., Grosan, C., "Evolving intrusion detection systems", *Genetic Systems Programming: Theory and Experiences*, 13:57-79, 2006

[12] Liu, Y., Chen, K., Liao, X., Zhang, W., "A genetic clustering method for intrusion detection", *Pattern Recognition*, 37, 2004

[13] Gassata, L.M., "A genetic algorithm as an alternative tool for security audit trails analysis ", *Int. Symposium in Recent Advances in Intrusion Detection*, 1998

[14] Wilson, D., Kaur, D., "Knowledge extraction from KDD'99 intrusion data using grammatical evolution", *WSEAS Transactions on Information Science and Applications*, 4:237-244, 2007

[15] Sen, S., Clark, J.A., "A grammatical evolution approach to intrusion detection on mobile ad hoc networks", *ACM Conferene on Wireless Network Security (WiSec)*, 2009

[16] Huang, Y., Fan, W., Lee, W., Yu, P.S., "Cross-feature analysis for detection ad-hoc routing anomalies", *Int. Conf. On Distributed Computinh Systems (ICDCS)*, 2003

[17] Sen, S., Clark, J.A., "Intrusion detection in mobile ad hoc networks", *Guide to Wireless Ad Hoc Networks*, chapter 17, pp. 427-454, 2009

[18] Vigna, G., Gwalani, S., Srinivasan, K., Belding-Royer, M., Kemmerer, R.A., "An intrusion detection tool for AODV-based ad hoc wireless networks", *IEEE Computer Security*, pp. 16-27, 2004

[19] Tseng, C., Wang, S. H., Lee, W., Ko, C., Lewitt, K., "Demem: distributed evidence driven message exchange intrusion detection model for MANET", Int. Symposium on Recent Advances in Intrusion Detection, 2006