DİNAMİK DEĞİŞEN PAKET İŞARETLEME OLASILIĞI YÖNTEMİNİ KULLANARAK İNTERNET PROTOKOL GERİ İZLEMESİ

Mustafa Sait ÖZEN

Yüksek Lisans Tezi

Elektrik-Elektronik Mühendisliği Anabilim Dalı

Temmuz - 2008

JÜRİ VE ENSTİTÜ ONAYI

Mustafa Sait Özen'in "**Dinamik Değişen Paket İşaretleme Olasılığı Yöntemini Kullanarak İnternet Protokol Geri İzlemesi**" başlıklı **Elektrik-Elektronik Mühendisliği** Anabilim Dalındaki, Yüksek Lisans Tezi 01.07.2008 tarihinde, aşağıdaki jüri tarafından Anadolu Üniversitesi Lisansüstü Eğitim-Öğretim ve Sınav Yönetmeliğinin ilgili maddeleri uyarınca değerlendirilerek kabul edilmiştir.

	Adı-Soyadı	**İmza**
Üye (Tez Danışmanı)	**: Yard. Doç. Dr. EMİN GERMEN**	**…..…….**
Üye	**: Yard. Doç. Dr. HAKAN G. ŞENEL**	**…..…….**
Üye	**: Yard. Doç. Dr. CÜNEYT AKINLAR**	**..…….**

Anadolu Üniversitesi Fen Bilimleri Enstitüsü Yönetim Kurulu'nun …… tarih ve …… sayılı kararıyla onaylanmıştır.

Enstitü Müdürü

ÖZET

Yüksek Lisans Tezi

DİNAMİK DEĞİŞEN PAKET İŞARETLEME OLASILIĞI YÖNTEMİNİ KULLANARAK İNTERNET PROTOKOL GERİ İZLEMESİ

Mustafa Sait ÖZEN

Anadolu Üniversitesi
Fen Bilimleri Enstitüsü
Elektrik-Elektronik Mühendisliği Anabilim Dalı

Danışman: Yard. Doç. Dr. Emin GERMEN
2008, 46 sayfa

Günümüz IP veri ağ alt yapısı, DDoS (Distributed Denial of Service) saldırılarının kaynaklarını belirlemekte yetersiz kalmaktadır. İnternet Protokolünün doğal yapısının anonim karakteristiğini azaltmak ve bu noktaların belirlenmeleri için IP geri izleme yöntemleri geliştirilmiştir. Bu tezde, IP geri izleme yöntemlerinden biri olan Olasılıksal Paket İşaretleme yöntemi üzerinde yoğunlaşılmış ve bu yöntemi geliştirmek için IP paketlerinin yönlendiricilere girdikleri ve çıktıkları noktalar arasındaki trafik yoğunluğu gözlemlenmiş ve buna bağlı olarak değişen paket işaretleme olasılığı önerilmiştir. Ayrıca paket işaretlerine zıplama sayıları eklenerek farklı saldırı yollarının tespit edilmesi amaçlanmıştır. Önerilen yöntemle literatürde tanımlanan yöntem, OPNET veri ağı benzetim yazılımıyla test edilmiş ve sonuçta daha az sayıda işaretlenmiş paket kullanarak saldırıların yönlendiricilere girdikleri noktaların bulunduğu gözlemlenmiştir.

Anahtar Kelimeler: İnternet Protokol Geri İzlemesi, OPNET, Olasılıksal Paket İşaretleme, Dinamik Değişen Paket İşaretleme Olasılığı

ABSTRACT

Master of Science Thesis

INTERNET PROTOCOL TRACEBACK BY USING DYNAMIC CHANGING PACKET MARKING PROBABILITY METHOD

Mustafa Sait ÖZEN

Anadolu University
Graduate School of Sciences
Electrical and Electronics Engineering Program

Supervisor: Assist. Prof. Dr. Emin GERMEN
2008, 46 pages

Nowadays, IP data network infrastructure is inadequate to find the origin of DDoS (Distributed Denial of Service) attacks. IP traceback algorithms are developed to abate the characteristic of anonymously available nature of the Internet Protocol and find the origins of these attacks. In this thesis, one of the IP traceback algorithms, Probabilistic Packet Marking is studied and the density of traffic between routers' ingress and egress points which IP packets enter and exit is used to develop a new method for the dynamic changing packet marking probability. Also hop number is added into packet marks to distinguish different attack paths. The proposed method and the method in the literature are tested by OPNET network simulation software and less number of marked packets is observed to be enough to find ingress points of routers concerning DDoS attacks.

Keywords: IP Traceback, OPNET, Probabilistic Packet Marking, Dynamic Changing Packet Marking Probability

TEŞEKKÜRLER

Öncelikle tez danışmanım Yard. Doç. Dr. Emin GERMEN'e sabrından, cesaretlendirmelerinden ve özellikle rehberliğinden dolayı teşekkür ederim. Yardımları olmasaydı bu çalışma asla olamazdı. Onunla çalışmak benim için bir zevkti. Ayrıca iş arkadaşlarım Reha Oğuz ALTUĞ, Safai TANDOĞAN ve Tevfik KIZILÖREN'e bana sağladıkları teknik destek ve tavsiyelerinden dolayı teşekkür ederim. Son olarak aileme ve hayatımdaki en güzel varlık olan Ebru'ya her zaman bana destek verdikleri için çok teşekkür ederim.

Mustafa Sait ÖZEN

Temmuz 2008

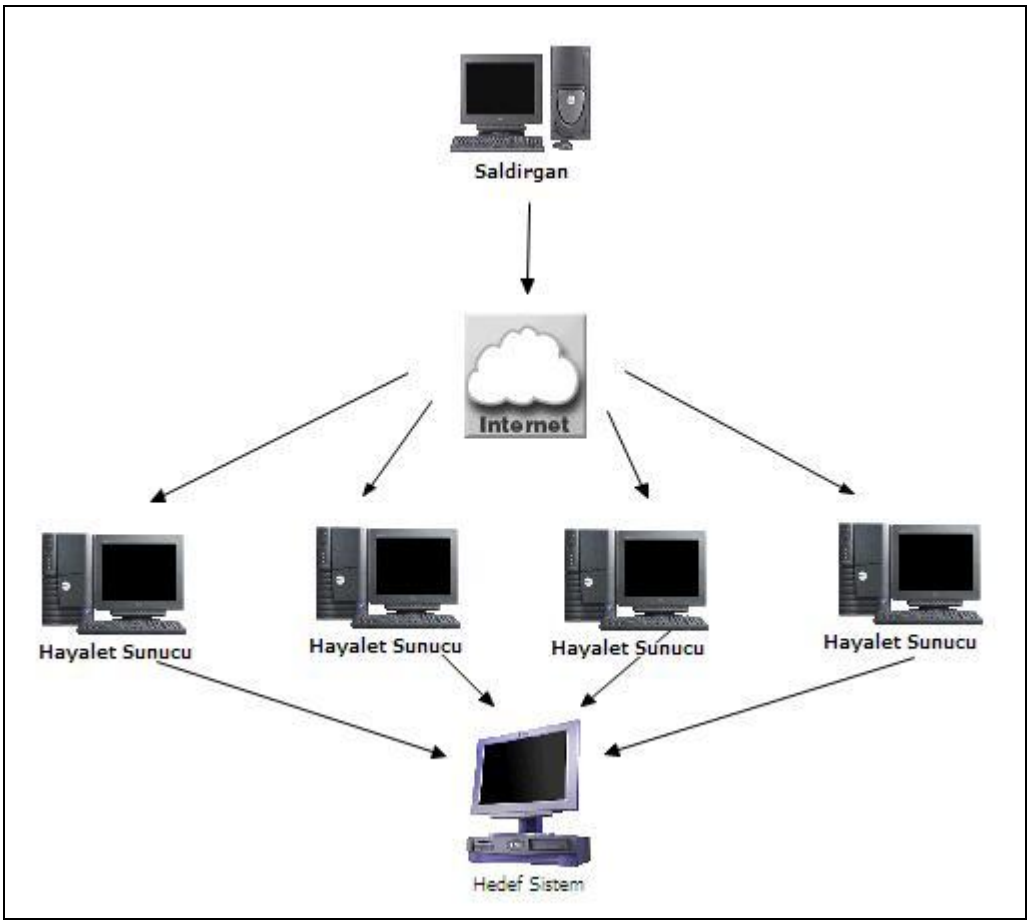
İÇİNDEKİLER

ŞEKİLLER DİZİNİ

ÇİZELGELER DİZİNİ

1. GİRİŞ

Günümüzde büyük ölçekli ağ sistemlerinde Servis Yıkımı (Denial of Service, DoS) ve/veya Dağınık Servis Yıkımı (Distributed Denial of Service, DDoS) saldırıları en önemli güvenlik sorunlarından biri haline gelmiştir. Bu saldırılar hem veri ağlarında gereksiz trafik yoğunluğunun artmasına neden olmakta hem de kurbanın veri ağını kullanımını oldukça olumsuz yönde etkilemektedir. Tüm bu saldırılar sonucu oluşan kayıplar veri ağı güvenliğinin sağlanmasının önemini günden güne arttırmaktadır. (D)DoS saldırılarının en temel amacı kullanıcıların var olan mantıksal ve fiziksel veri ağı kaynaklarına ulaşmalarını bir şekilde engellemektir. DoS saldırıları veri ağında tek bir çıkış noktası kullanılarak yapılmaktayken DDoS saldırıları (Şekil 1.1. DDoS Saldırısı) birden fazla saldırı noktası ve değişik rotalar kullanılarak yapılır. Her iki tür saldırı da veri ağının performansını düşürmektedir ve doğal olarak her iki durumda da saldırganlar kendi kaynaklarını gizlemek istemektedirler. Günümüz veri ağı alt yapısında bir IP paketi varacağı noktaya ulaşana kadar sadece varış IP adresine bakılmaktadır. Eğer bu paketle gelecek bilgiye karşılık olarak bir cevap gönderilecekse o zaman kaynak IP adresine ihtiyaç duyulmaktadır. Saldırı sırasında saldırgan kendini gizlemek istediğinden IP Adres Spoofing tekniği ile saldırı paketlerinin kaynak adreslerini değiştirir. Kaynak IP adresi değiştirilmiş saldırı paketleri incelendiğinde kaynak IP adresine bakarak saldırının gerçek kaynağını bulmak günümüz teknolojisiyle neredeyse olanaksızdır. Saldırı paketlerinin izledikleri yolları veya veri ağına giriş noktalarını belirlemek amacıyla literatürde birçok yöntem önerilmiştir. IP kaynak adresini kontrol etmeden gerçek kaynak IP adresini bulmaya yönelik araştırmalar İnternet Protokol Geri İzleme (Internet Protocol Traceback) yöntem bilimleri altında sınıflandırılmışlardır.



Şekil 1.1. DDoS Saldırısı

Günümüzün internet altyapısı zararlı saldırıları bertaraf edebilecek uygun bir savunma sağlayamamasından dolayı, farklı birçok yöntem kullanıcıları korumak için geliştirilmiştir. Paketlerin yönlendirici üzerindeki durumlarının kaydedilmeden dolaşmaları, IP paket başlığının değiştirilebilmesi saldıran veya saldırganlara farklı türde etkili ve zararlı saldırılar düzenlemelerine olanak sağlamaktadır. Saldırıya maruz kalan sistemlerde yapılması gerekli iki temel işlem vardır. Bunlardan birincisi çok geç olmadan saldırıyı algılamaktır. Zorlama Algılama Sistemleri (Intrusion Detection Systems, IDSs) bu sorunu çözmek için çabalamaktadırlar. İkinci işlem ise veri ağındaki saldırının kaynağını bulmak veya saldırı paketlerinin gerçek kaynağını belirlemektir. IP Geri İzlemenin temel amacı saldırı paketlerinin asıl kaynağının kimliğini belirlemektir. Saldırı yapan bilgili kişi veya kişiler saldırıları kendi bilgisayarlarından yapmak yerine farklı kişilere ait bilgisayarları kullanarak ta yapabilmektedirler. Bu bilgisayarlara sahip olan kişi veya kişiler bu bilgisayarın saldırı için kullanıldığından haberleri bile

olmayabilir. Saldırganlar bu bilgisayarlara kurdukları tespit edilmesi çok zor olan hayalet programlar (daemon) sayesinde DDoS saldırılarını gerçekleyebilmektedirler. Bu yazılımların kurulu olduğu bilgisayara hayalet sunucu adı verilir. Eğer saldırılar hayalet sunucular kullanılarak ve/veya IP paketlerinin kaynak adreslerini değiştirerek yapılırsa saldırı paketlerin IP datagram başlıklarına bakarak saldırının giriş noktasını belirlemek olanaksız hale gelir.

Saldırıların kaynağını bulmak, gerek kullanıcı açısından gerekse ağ yönetimi yönünden hayati öneme sahiptir. Dolayısıyla zararlı paketlerin çıkış noktalarının bulunması ve ayrıca bu paketlerin ağ içindeki hareketlerinin belirlenmesi için literatürde çok çeşitli yöntemler karşımıza çıkmaktadır.

Bu tezde, Olasılıksal Paket İşaretleme (Probabilistic Packet Marking, PPM) tabanlı bir IP Geri İzleme yöntemi geliştirilmiştir. Bu yöntemle yönlendirici cihazlarında IP paketleri veri ağı trafiğine bağlı olarak değişen olasılıkla işaretlenmektedir. Böylece saldırı sırasında paket trafiği artacağından saldırı yollarındaki işaretlenmiş saldırı paket sayısı da artmış olacaktır.

Tezin ikinci bölümünde, (D)DoS saldırıları ile İnternet protokol geri izlemesinin gerekliliği ve başlıca yöntemleri açıklanırken, üçüncü bölümde geliştirilen yeni PPM yöntemini benzetim yapmak (simulation) için kullanılan OPNET veri ağları simülasyon programı anlatılmıştır. Dördüncü bölümde önerilen yöntem etraflıca anlatılmış ve bu yöntemle yapılan simülasyon sonuçları sunulmuştur. Beşinci ve son bölümde ise elde edilen sonuçlar literatürdeki diğer yöntemlerle karşılaştırılmış ve gelecekteki olası çalışmalar hakkında öneriler belirtilmiştir.

2. İNTERNET PROTOKOL GERİ İZLEMESİ

DoS saldırısının amacı veri ağları kullanılarak yapılan bir servisin asıl kullanıcılarının o servisin kaynaklarını kullanmalarını engellemektir [1]. Servisin sürekli ve sorunsuz kullanımını engellemek için çok çeşitli yollar vardır. Bunlardan biri var olan veri ağındaki trafik yoğunluğunu arttırmak ve bu sayede normal trafiği engellemektir. Bir diğeri, servis veren ve servis alan bilgisayarlar arasındaki bağlantıyı koparark servisin sağlanmasını engellemektir. Diğer bir tanesi ise belli kullanıcıların servise ulaşmasını veya servisin özel bir kişiye ya da sisteme ulaşmasını engellemektir.

Günümüzde DoS saldırılarını engellemek çok önemli bir araştırma konusu haline gelmiştir. Bunun sebebi ise yapılan saldırıların amacının hedef bilgisayar sistemlerini ve/veya veri ağlarını kullanılamaz hale getirmek olmasıdır. DoS saldırıları genellikle bir saldırı noktası ve bir veri ağı yolu kullanılarak yapılmaktayken Dağınık Servis Yıkımı (DDoS) saldırıları ise birden fazla saldırı noktasından farklı veri ağı yolları kullanılarak yapılmaktadır. DDoS saldırıları yoğunluklarından dolayı DoS saldırılarından çok daha tehlikeli ve zararlıdır. Yapılan saldırılar büyük çapta maddi hasarlara sebep olmaktadır. Yahoo[1] 7 Şubat 2000 tarihinde DDOS saldırısına maruz kalmıştır [2]. Analistlerin tahminine göre servis verilemediği 3 saat boyunca Yahoo'nun toplam zararı çok fazladır.

DDoS saldırıları daha önceki bölümde de anlatıldığı gibi hayalet sunucular kullanılarak yapılmaktadırlar. Öncelikle saldırgan veya saldırganlar ele geçirdikleri farklı bilgisayarlara "daemon" adı verilen hayalet yazılımlar kurarlar. Hayalet yazılımların kuruldukları bilgisayarların genel özellikleri ise yüksek miktarda ağ trafiği üretebilen Web, E-Posta, FTP gibi sunucular olmalarıdır. Bu sunuculara bağlanan noktaların sayısı çok fazla olduğundan dolayı saldırgan ile aralarındaki bağlantının tespit edilmesi çok zordur. Hayalet yazılımların kurulduğu bu bilgisayarlara hayalet sunucular adı verilir. Saldırgan veya saldırganlar hayalet sunucularının bir listesini tutarlar. Saldırının yönetildiği bilgisayarlardan listedeki hayalet sunuculara saldırıyı başlatmak için komut gönderilir. Bu komutta saldırının nereyi hedef alacağı bilgisi vardır. Eş zamanlı

[1] http://www.yahoo.com

olarak hayalet sunucular hedef sisteme saldırmaya başlar. Saldırılar hayalet sunucular tarafından yapıldığından arka planda saldırıyı organize eden saldırgana ulaşmak saldırı sırasında olanaksız hale gelir. Hayalet sunucular belirlenip incelendiğinde saldırının yönetildiği noktanın bulunması çok zordur. Çünkü kurulan hayalet yazılımlar otomatik olarak çalışmaktadır ve saldırganın bilgisayarıyla daima bir bağlantı kurmalarına gerek yoktur.

(D)DoS saldırılarından korunmak için bazı yöntemler önerilmektedir. Süzgeçler [3], yerel internet sağlayıcının dışarıdan gelen ve iç ağ yapısına ait olan kaynak adresli IP paketlerinin içeriye girmesini ve/veya içeride oluşturulan ve dış ağlara ait kaynak adresli IP paketlerinin dışarıya çıkmalarını engellemeyi amaçlamaktadırlar. Bu süzgeçler tüm internet servis sağlayıcıları tarafından kullanılırlarsa ancak o zaman geçerli bir çözüm elde edilebilir ve kaynağı belirsiz paket trafiği son bulabilirdi. Bir diğer yöntem ise Zorlama Algılayıcı Sistemlerdir (Intrusion Detection Systems, IDSs) [4]. IDSs'lerin amacı ise çok geç kalmadan saldırı olduğunu algılamaktır. IDS saldırı algıladığında gerekli kişileri veya güvenlik sistemlerini uyarır. Bu sayede çok geç olmadan saldırının bertaraf edilmesi için önlemler alınabilir.

Saldırının engellenmesi kadar saldırıyı gerçekleyen kişi ve kişilerin bulunması çok büyük önem taşımaktadır. Saldırıdan kaynaklanan maddi hasarlardan dolayı saldırganlar suç işlemiş duruma düşerler. Eğer bu kişi veya kişiler tespit edilirseler haklarında kanuni işlemler yapılabilir. Daha öncede bahsedildiği gibi (D)DoS saldırıları kaynak adresi değiştirilmiş IP paketleri veya hayalet sunucular kullanılarak yapılmaktadır. İnternet Protokolünün doğal yapısının anonim karakteristiğini azaltmak ve IP paketlerinin gerçek kaynaklarını belirlemek için İnternet Protokol Geri İzleme yöntemleri önerilmektedir.

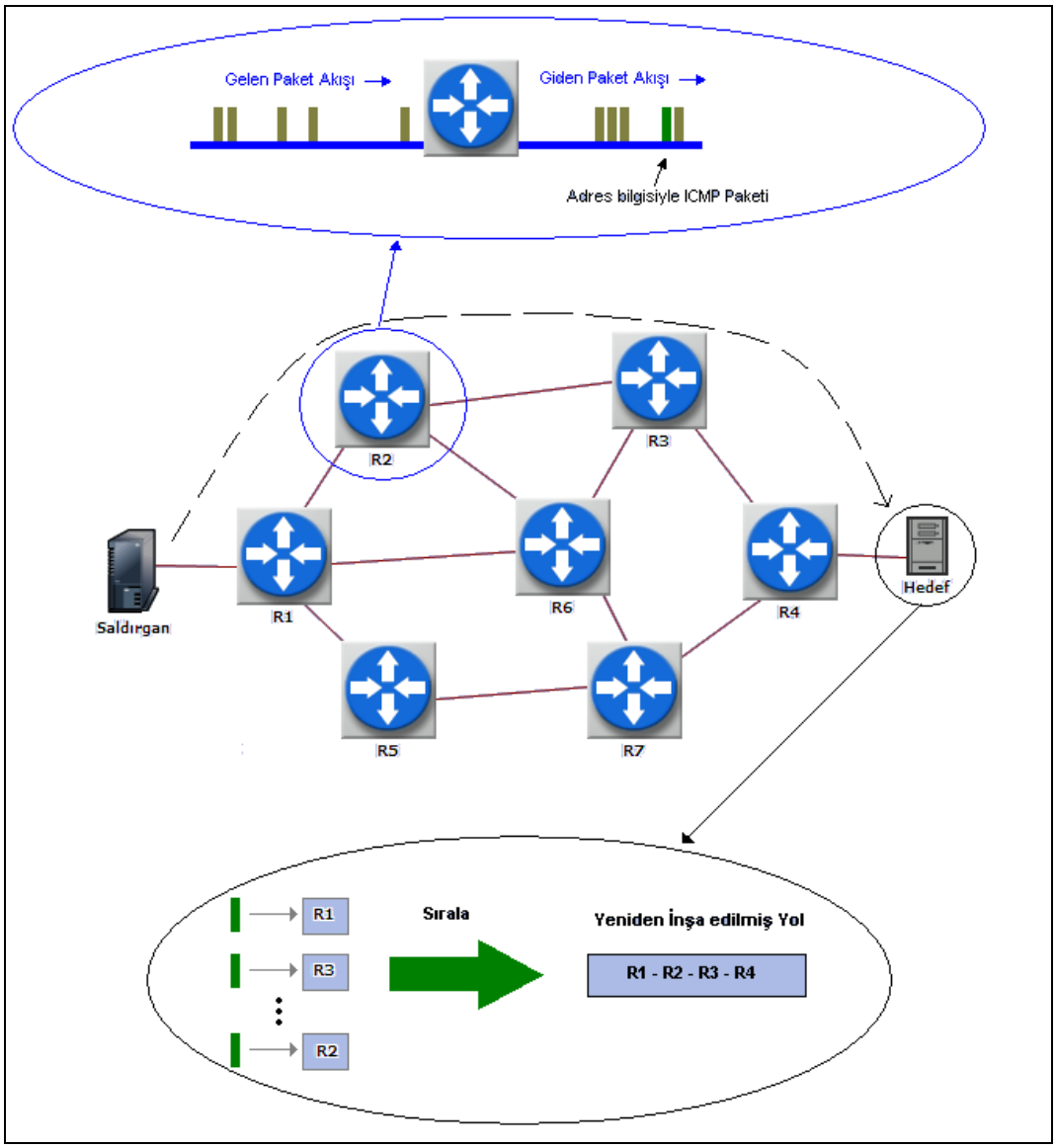
IP Geri İzlemesi ilk olarak Savage et. al. [5] tarafından önerilmiştir ve bu öneri üzerine birçok farklı yöntem geliştirilmiştir. Bu yöntemleri sınıflandırmak istenilirse dört ana başlık altında bu yöntemler incelenebilir: Mesajlaşma (Messaging) [6], Günlük Tutma (Logging) [7], Bağlantı Testi (Link Testing) [8], Paket İşaretleme (Packet Marking).

2.1. Mesajlaşma (Messaging)

İnternet Protokol Geri izleme tekniklerinden bir tanesi mesajlaşma tekniğidir. Bu yöntemin temel çıkış noktası yönlendirici cihazların IP paketlerini geri izlemek için İnternet Kontrol Mesaj Protokol (Internet Control Message Protocol, ICMP) mesajlarını kullanmalarıdır. Mesajlaşma yöntemi Şekil 2.1.'de gösterilmektedir. Mesajlaşmanın kullanıldığı veri ağındaki yönlendirici cihazlar, kendilerine gelen paketler içerisinden belli bir olasılıkla bir paket seçerler ve seçilen paketin kaynağına ICMP Geri İzleme Mesajı (iTrace) üretirler. Paket seçme olasılıkları ağ yapısına göre deneysel belirlenebildiği gibi ayrıca genelde her 20.000 pakette bir tane olacak şekilde önerilmiştir [6]. iTrace mesajların içeriğinde bir önceki ve bir sonraki hop bilgileri ile yaşam süresi (TTL) bilgisi vardır. Bu mesaj oluşturulurken TTL değeri 255 olarak atanır. TTL değeri kaynağa doğru giderken üzerinden geçtiği her noktada bir azaltılır. Bu değer daha sonra geri izleme işleminde yönlendirici cihazların saldırı yolundaki sırasını bulmak için kullanılmaktadır

(D)DoS saldırısı sırasında hedef noktaya giden paket sayısı aşırı derecede artacağı varsayıldığından, hedef bilgisayar saldırının gerçeklendiği rota üzerindeki mesajlaşma yöntemini kullanan tüm yönlendirici cihazları tespit edebilecektir. Saldırı sırasında elde edilen bilgiler kullanılarak saldırının üzerinden geçtiği yönlendiriciler belirlenir ve TTL bilgileri kullanılarak tespit edilen yönlendiriciler arasında sıralama yapılır. Bu sıralama sonucunda saldırı yolları belirlenir.

Mesajlaşma tekniğinin dezavantajlarından biri internet trafiğini arttırmasıdır. Saldırı esnasında gelen paket sayısı artacağından seçilen paketlerin kaynağına gönderilen iTrace mesajlarının sayısı da artacaktır. Bu trafik artışını azaltmak amacıyla paket seçme olasılığı azaltıldığı zaman ise doğru saldırı kaynağını bulmak için ihtiyaç duyulan paket sayısı artmaktadır.



Şekil 2.1. Mesajlaşma (Messaging)

2.2. Günlük Tutma (Logging)

Günlük Tutma, veri ağlarında dolaşan IP paketlerini kayıt altına alarak İnternet Protokol Geri izleme yapmayı amaçlayan bir yöntemdir. Günlük Tutmanın ana fikri ise gelecekte yapılacak analizler için merkezi sunucularda veri ağlarındaki trafiğin kaydedilmesidir. Ağ üzerindeki olası tüm trafiğin yarattığı bilgilerin saklanması çok ciddi bir yük getireceğinden sunucularda bilgiler olasılıksal örnek alma veya özetlenmiş veri saklama yöntemleri kullanılarak depolanmaktadır. Bu yöntemin kullanıldığı veri ağlarında bir tek saldırı paketi bile o paketin asıl kaynağının bulunmasına için yeterli olmaktadır. Günlük Tutma

yönteminin kullanılabilmesi için veriyi çok hızlı bir biçimde depolayabilen yüksek kapasiteli hafıza disklerine sahip sunuculara ihtiyaç duyulmaktadır. Ayrıca bu yöntem, yönlendirici cihazlara gelen paketler için hesaplama yükü getirmektedir. Bu yük tüm veri ağı trafiğinde genel bir gecikmeye yol açmaktadır.

Günümüz teknolojisini düşünülürse büyük ölçekli bir veri ağındaki internet trafiğini senkronize olarak kayıt altına alabilecek hızda ve kapasitede bir disk yapısı yoktur. Ağdaki trafiği kaydeden sunucuda oluşabilecek bir veri depolama sorununda ise Günlük Tutma işleminin ne kadar doğru sonuç verebileceği ise tartışmalı bir konudur. Tüm bu olumsuzluklar bu tekniğin var olan veri ağları altyapısında kullanılabilmesini güç hale getirmektir [7].

2.3. Bağlantı Testi (Link Testing)

Bağlantı testi işlemi tüm olası bağlantıların kontrol edilerek saldırı paketlerinin kaynağını belirlemek üzerine kurulmuş bir IP Geri İzleme yöntemidir. Bu yöntemin mevcut protokollar kullanılarak uygulanması çok zor değildir. IP Geri izlemesi yapacak nokta, kendine en yakın yöneltici cihazdan başlayarak trafiğin akış yukarısına doğru bağlantıları test ederek kaynak adresi bulmayı amaçlamaktadır. Günümüz veri ağı altyapısı bu geriye doğru izleme işlemine olanak sağlamaktadır. Bu yöntem geri izleme işlemi sırasında saldırının devam ettiği kabul edilerek geliştirilmiştir. Bağlantı Testi, IP paketlerinin kaynaklarını bulmak için zamana ihtiyacı vardır. Eğer saldırı periyodu geri izleme işleminden daha kısa ise giriş noktasının bulunması olanaksızdır. Kısa sürelerde yapılan (D)DoS saldırılarında Bağlantı Testi yöntemi kullanışsız hale gelmektedir. Bu yöntemin kullanıldığı veri ağ yapılarını bilen saldırgan veya saldırganlar bu yapılara karşı yapılacak (D)DoS saldırılarını kısa sürede olacak şekilde düzenlerlerse gerçek saldırı kaynaklarını bulmak olanaksız hale gelir. Bu yöntem iki farklı varyasyonda incelenebilir: Giriş Hata Ayıklama (Input Debugging), Kontrollü Sel (Controlled Flooding).

2.3.1. Giriş Hata Ayıklama (Input Debugging)

Birçok yönlendirici cihazın çıkış noktalarındaki belirli IP paketlerinin hangi giriş noktasından girdikleri belirleyebilen *giriş hata ayıklama* özelliği vardır. Bu yöntemin kullanılması birkaç ardışık adımı içermektedir. Öncelikle

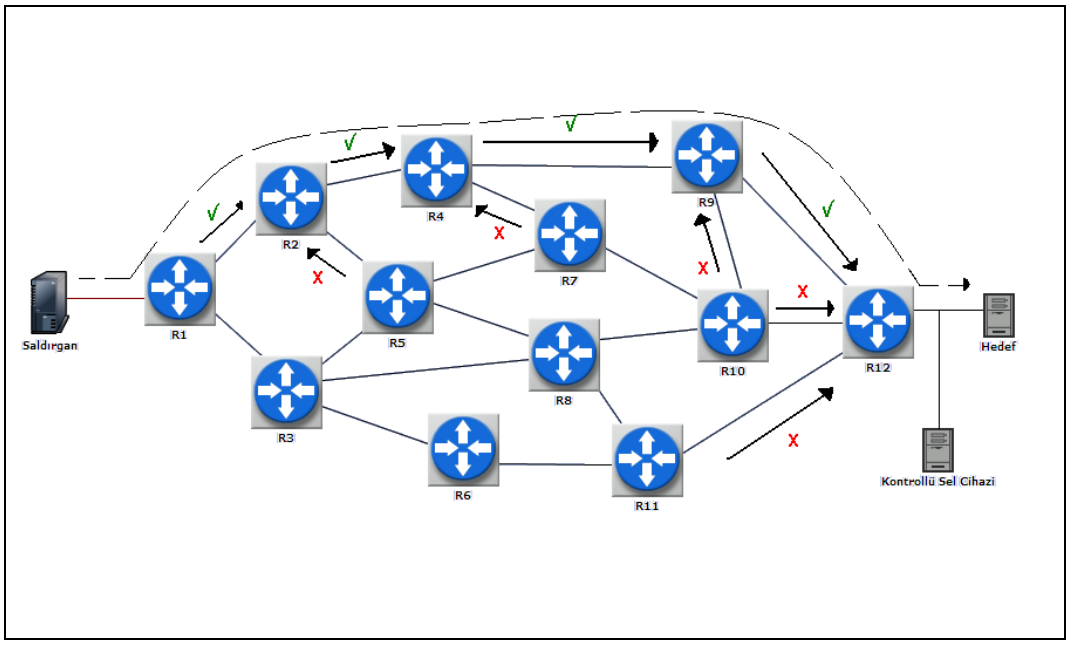
saldırıya hedef olan bilgisayarın yöneticisi IDSs kullanarak saldırı olduğunu algılar. Gelen tüm saldırı paketlerindeki mevcut genel bir karakteristik özellik belirleyerek bir *saldırı imzası* geliştirir ve bu imzayı ağ yöneticisine iletir. Daha sonra ağ yöneticisi hedef bilgisayarın bağlı olduğu yönlendirici cihazın bağlantı noktasında saldırı imzası olan paketlere Giriş Hata Ayıklama işlemini uygulayarak paketlerin hangi yönlendirici giriş noktasından girdiğini bulur. Sırasıyla bu noktanın bağlı olduğu diğer yönlendirici cihazda da bu işlem yapılarak saldırının kaynağın bulunması hedeflenmektedir. Bu işlem tüm ağ içerisinde özyinelemeli (recursive) olarak akışın ters istikametinde uygulanarak saldırının asıl kaynağı bulunana kadar devam eder.

Bu yöntemin en büyük dezavantajlarından birisi saldırının kaynağının veri ağının dışında ve ağ yöneticisinin inceleme olanağı olmadığı bir yerde olduğu durumda karşımıza çıkmaktadır. Böylesi bir durumda yöntemden sonuç elde edilemeyecektir. Giriş hata ayıklama yöntemi ağ yöneticisi tarafından ara sıra manüel olarak yapılırken, bazı internet servis sağlayıcıları bu işi otomatik yapabilmek için araçlar geliştirmişlerdir [9].

Tüm İnternet sağlayıcıların bu yöntemi kullandığını var sayarsak saldırı sırasında aralarındaki koordinasyonun sağlanması ve geri izleme işlemin yönetilmesi çok açık bir sorundur. Yöntemin sağlıklı çalışabilmesi için tüm ağ yöneticilerinin giriş ayıklama sistemini yapabilecek kapasitede olması ve saldırı sırasında sistemlerine müdahale edebilecek konumda bulunmaları gereklidir. Bu sebeplerden dolayı bu yöntem yerel bir veri ağı yapısında kullanılmaktan öteye gidememektedir.

2.3.2. Kontrollü Sel (Controlled Flooding)

Kontrollü Sel yöntemi ilk olarak Burch ve Cheswick tarafından önerilmiştir [8] ve yapısından dolayı sadece DoS saldırı için kullanılabilen bir yöntemdir. Kontrollü Sel, DoS saldırısı sırasında saldırı bağlantıları aşırı yükleneceğinden bu bağlantılar kontrol edilerek saldırının kaynağının bulunabileceği fikri üzerine kurulmuştur.



Şekil 2.2. Kontrollü Sel (Controlled Flooding)

Kontrollü Selin çalışma prensibi Şekil 1-4'de gösterilmiştir. Şekle göre (D)DoS saldırısı R1 -> R2 -> R4 -> R7 -> R9 -> R12 rotası kullanılarak gerçekleşmektedir. Saldırının hedefi olan nokta, saldırıyı algıladıktan sonra Kontrollü Sel Aracını kullanarak saldırının asıl kaynağını bulmak için geri izleme işlemine başlar. Kontrollü Sel Aracı yönlendirici cihazlara bağlanarak chargen [10] adı verilen servisi başlatır. Yönlendirici chargen servisi başlatan kaynağın TCP veya UDP'nin 19. kapısını kullanarak kaynağa çok büyük miktarlarda verinin gitmesini sağlar. Saldırı hedefinin bağlı olduğu yönlendirici olan R12 seçilerek bu yönlendiriciye bağlı olan R9, R10 ve R11 yönlendiriciler arasındaki bağlantılar test edilir. Test işlemi Kontrollü Sel Aracı tarafından yapılır. Kontrollü Sel Aracı R9, R10 ve R11 yönlendiricilerin chargen servislerini sırayla başlatır. Chargen servisini başlatan cihaza çok miktarda veri akışı olacağından Kontrollü Sel Aracı servisi başlatmak için gönderdiği IP paketlerinin kaynak adreslerini IP Spoofing yöntemiyle R12'in arabirim IP adresleriyle değiştirir. Bu sayede veri akışları R12 üzerine yapılır. Saldırının geçtiği bağlantılarda oluşturulan veri akışındaki paket düşme oranının yüksek olacağı kabul edilerek yapılan bu testlerde R12 ile R9 arasında paket düşme oranı diğerlerine göre daha yüksek olacaktır. R12 ile R9 arasındaki bu bağlantı yolu saldırının izlediği yol olarak

kabul edilerek aynı işlemler R9 yönlendiricisi için de yapılır. Özyinelemeli olarak tekrar eden işlemler sonucunda saldırı noktası bulunur.

Kontrollü Sel'in mevcut veri ağlarında uygulanması için birkaç engel bulunmaktadır. Bunlardan birincisi çoğu yönlendiricinin chargen servisinin kapalı olmasıdır. İkincisi geri izlemeyi yapacak bilgisayarın, izleme yapacağı veri ağındaki yönlendiricilerin tüm arabirim adreslerini biliyor olması gereklidir. İnternet servis sağlayıcıların, yönlendiricilerinin arabirim adres bilgilerini müşterileri ile paylaşıp paylaşmayacağı ayrı bir sorun teşkil etmektedir. Önceden de bahsedildiği gibi Kontrollü Sel sadece DoS saldırıları için kullanılabilir. Hedef noktanın bu yöntemi kullanabilmesi için öncelikle saldırının DoS mu yoksa DDoS mu olup olmadığının belirlemesi gereklidir. Bunun nasıl yapılacağı ise ayrı bir sorundur. DDoS gibi daha zararlı ve etkili saldırı türü için kullanılamaması Kontrollü Sel'in kullanılabilirliğini azaltmaktadır.

2.4. Paket İşaretleme (Packet Marking)

Paket işaretlemenin amacı, veri ağlarında IP paketlerinin yönlendiriciler arasında dolaşımı sırasında yönlendiricilere ait kimlik bilgilerin bu paketlere eklenmesi ve saldırı sırasında veya sonunda saldırıdan etkilenen hedef sistemin bu işaretleri paketlerden toplayarak ve bunları kullanarak saldırı akışını veya akışlarını tespit etmektir. Bu yöntem yönlendiricilere donanımsal olarak hiç bir yük getirmezken yazılımsal olarak getireceği yük oldukça düşük düzeydedir. Paket işaretleme işlemi yönlendiriciler tarafından temel görevleri olan paket yönlendirilme işlemini bozmayacak şekilde yapılması gerekmektedir. Yönlendiricilere fazla hesaplama yükü eklememesine rağmen, işlem yükünün çoğunluğu geri izleme işlemi sırasında hedef nokta tarafından yapılır. Paketlerin içindeki işaretlerin toplanması ve bunlarla ilgili hesaplanmaların yapılması için hedef bilgisayarlarda hafıza ve işlem gücüne ihtiyaç duyulmaktadır. Günümüz bilişim teknolojisinde gelinen nokta göz önünde bulundurulduğunda hemen her saldırıya maruz kalacak önemdeki bilgisayarın da böyle bir güce sahip olduğu varsayımı yanlış bir varsayım değildir.

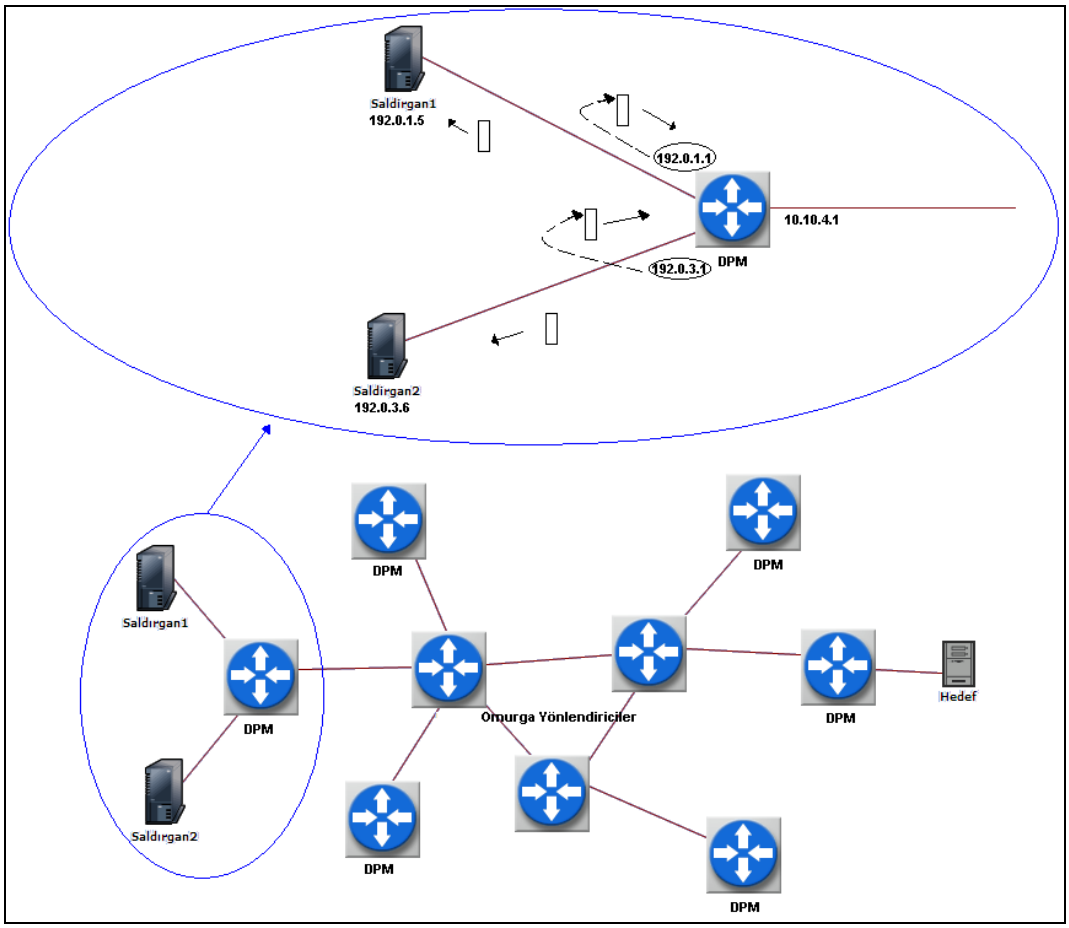
Paket işaretleme yönteminin kullanılabilmesi için mevcut veri ağ altyapısını ek bir donanım eklenmesi gerekli değildir. Tamamen yazılımsal olan

bu yöntem için yönlendiricilerde yazılım güncelleştirmesi yapılması yeterlidir. (D)DoS saldırılarına maruz kalabilme ihtimali olan noktalara ise paketlerdeki işaretleri kullanarak IP Geri İzlemesi yapabilecek yazılımların yüklenmesi yeterli olacaktır.

Paket İşaretleme yöntemi paket işaretleme yaklaşımına göre iki farklı türde yapılmaktadır: Rast Gele Olmayan Paket İşaretleme [11] (Deterministic Packet Marking, DPM), Olasılıksal Paket İşaretleme (Probabilistic Packet Marking, PPM).

2.4.1. Rast Gele Olmayan Paket İşaretleme (Deterministic Packet Marking)

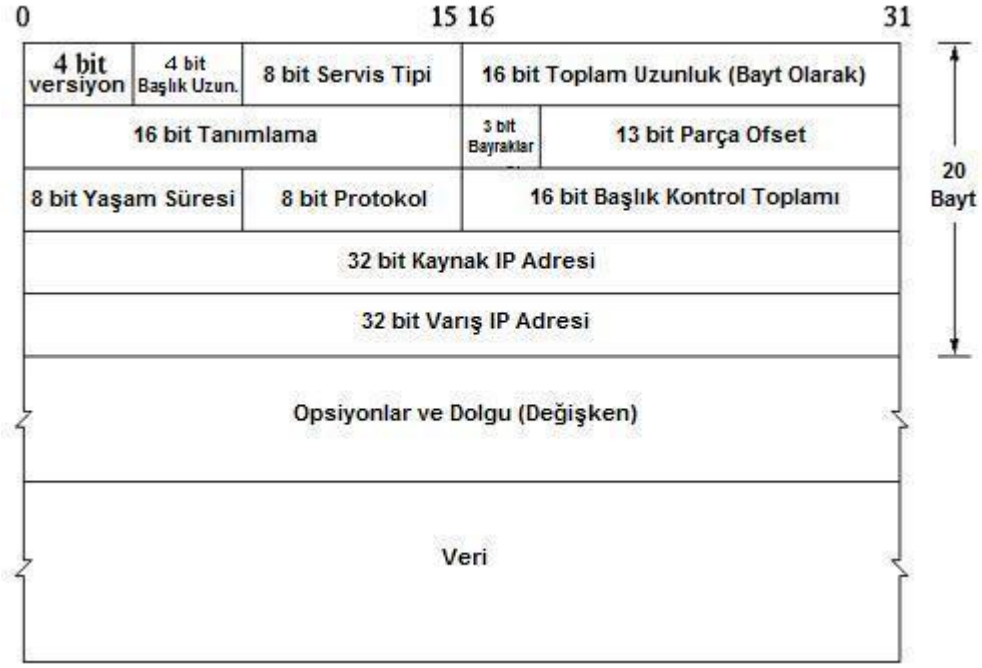
Rast Gele Olmayan Paket İşaretleme (Deterministic Packet Marking, DPM) ilk olarak Andrey Belenky ve Nirwan Ansari tarafından önerilmiştir [11]. Bu yöntemi kullanan yönlendiriciler gelen paketleri belli bir olasılığa bağlı olarak işaretlemek yerine gelen tüm paketleri işaretlemektedirler. Yöntemin en önemli handikaplarından birisi IP Geri İzleme yöntemi hakkında bilgili kişi veya kişilerin paketlerdeki işaretleri değiştirme ihtimalleri olmasıdır. DPM yönteminde tüm paketler yönlendiriciye geldikleri her seferde işaretlendiği için paket işaretleri değiştirilmiş paketler tekrar doğru işaretler ile işaretlenir. DPM yönteminde paket işaretleme işlemi Şekil 2.3.'te gösterildiği gibi kenar yönlendiriciler (edge routers) tarafından yapılır.



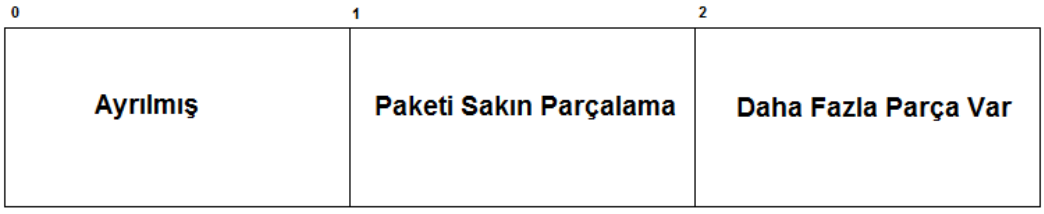
Şekil 2.3. Rast Gele Olmayan Paket İşaretleme (Deterministic Packet Marking)

DPM, IP Datagram'ın [12] 16 bitlik Tanımlama Alanı (Identification Field) (Şekil 2.4.) ve 1 bitlik Ayrılmış Bayrağı (Reserved Flag) (Şekil 2.5.) kenar yönlendirici cihazların giriş arabirim adreslerini paketlere işaretlemek için kullanan bir yöntemdir. İşaretleme işi bu yöntemin kullanıldığı veri ağı yapısındaki kenar yönlendirici cihazlarının görevidir. DPM'in uygulandığı veri ağında omurga yönlendirici cihazları işaretleme yapmazlar. Bu sayede işaretlenen paketler varış noktalarına ulaşan kadar kenar yönlendiriciler tarafından eklenen işaretleri değiştirilmez ve hangi kenar yönlendirici ile işaretlendikleri bilgileri kaybedilmez. İşaretlemeyi yapan yönlendiricinin giriş ara yüz adresini bulabilmek için 32 bitlik IP adres alanı gerektiğinden, DPM 32 bitlik yönlendirici ara yüz adresini 16 bit uzunluğunda üst 16 bitlik kısım ve alt 16 bitlik kısım olmak üzere iki ayrı parçaya ayırır. Kenar yönlendirici cihazında hangi parçanın Tanımlama alanına ekleneceği rast gele belirlenir. Ayrılmış Bayrak hiç kullanılmadığından dolayı rastsal yapılan kısım seçiminin sonucu buraya yazılır. Üst 16 bitlik kısım

eklenmiş ise Ayrılmış Bayrağa “1” yazılırken alt 16 bitlik kısım eklendiyse ‘0’ yazılır. Saldırı sırasında kurban, gelen paketlerdeki 16 bitlik kısımları ayrılmış bayraktaki değerlere bakarak iki ayrı tabloda saklar. Her iki tablodaki 16 bitlik kısımlar eşleştirilip 32 bitlik kenar yönlendirici IP adresleri bulunur. Bu adresler kullanılarak saldırı giriş noktaları bulunur. Bu yöntemin dezavantajı ise DPM kullanan tüm yönlendirici cihazlarının gelen her paketi işaretlemek için kullandığı hesap yüküdür. Ayrıca paket işaretleme işlemi kenar yönlendirici cihazları tarafından yapıldığından omurga yönlendiriciye bağlı saldırgan veya saldırganlar için geri izleme yapmak olanaksızdır. Bu yöntemle sadece (D)DoS saldırıların giriş noktaları belirlenebilmektedir.



Şekil 2.4. IP Datagram

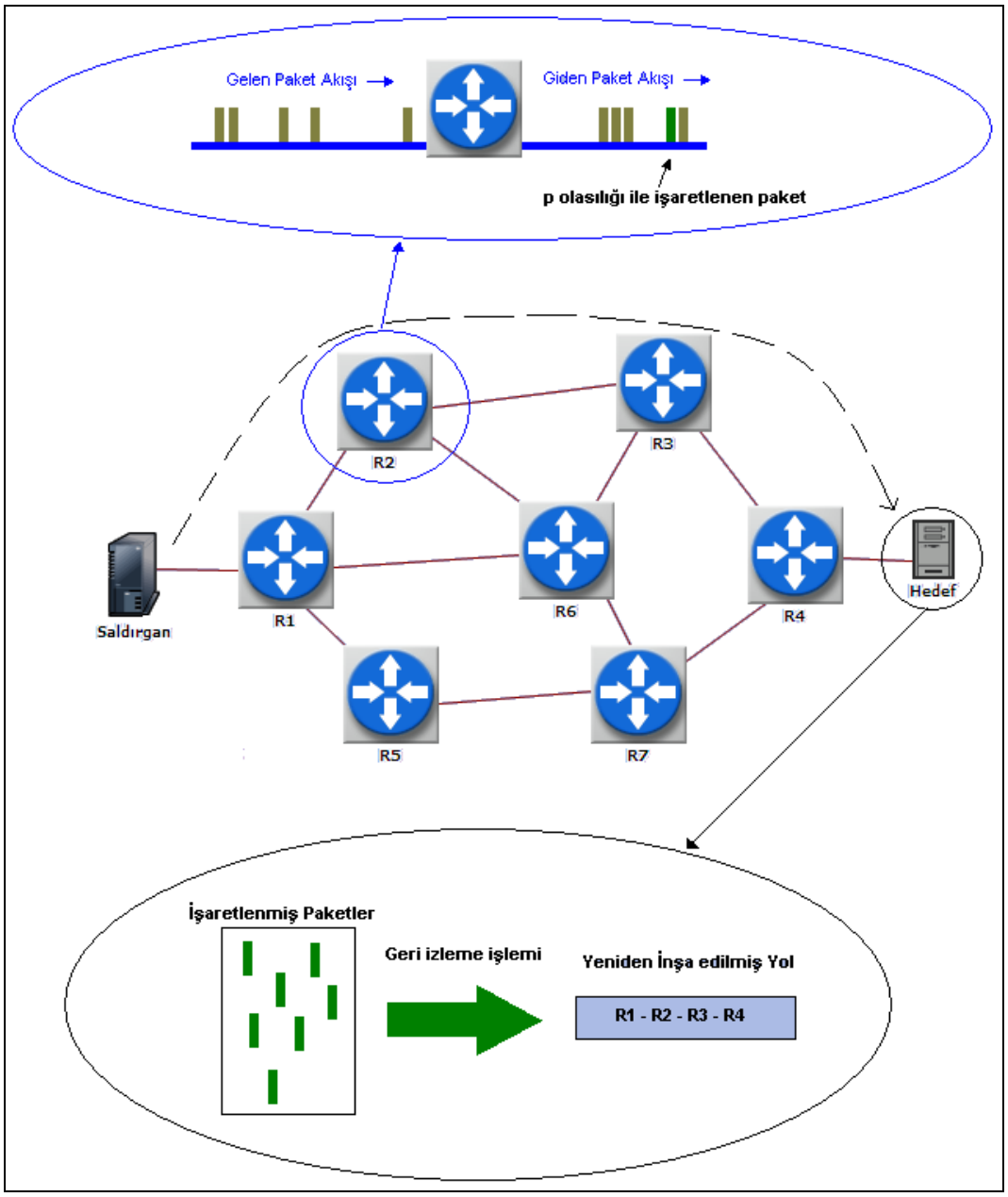


Şekil 2.5. Bayraklar (Flags)

2.4.2. Olasılıksal Paket İşaretleme (Probabilistic Packet Marking)

Olasılıksal paket işaretleme (Probabilistic Packet Marking, PPM) ilk olarak Burch ve Cheswick [8] tarafından önerilmesine rağmen Savage et. al. [5] tarafından ortaya atılmıştır. PPM'in amacı yönlendirici cihazlar tarafından rasgele işaretlenen IP paketleri kullanılarak zararlı trafiğin rotasını belirlemektir. Yöntem iki kısımdan oluşmaktadır. Birinci kısım internet üzerinde yol alan IP paketlerinin yönlendirici cihazlarının üzerinden geçerken düşük bir olasılıkla işaretlenmesidir. İkinci kısım ise saldırıdan etkilenen hedefin IP paketlerindeki işaretleri toplayarak saldırı rotasını yeniden oluşturmasıdır.

PPM yöntemini kullanan yönlendirici cihazları işaret olarak giriş ara yüzü IP adreslerini kullanmaktadırlar. IP Versiyon 4 (IPv4) ara yüz adresleri 32 bit uzunluğundadır. Paket işaretin IP paketine eklenmesi paketin boyutunu arttırmaktadır. Bu ek yük PPM metodunun dezavantajlarından biridir. Paket boyutunu azaltmak amacıyla çeşitli yöntemler geliştirilmiştir [13]. Bant genişliğini azaltmak için paket işaretleme olasılığı küçültülür ise saldırı rotasını bulmak için gereken işaretlenmiş IP paket sayısı artmaktadır. Savage et. al. 1/20000 olasılıkla paket işaretlemeyi önerdiği halde bu olasılıkla doğru saldırı rotasının 95% doğruluk oranıyla belirlenmesi için en az 294.000 pakete ihtiyaç duyulmaktadır [5]. [13]'te geliştirilen yöntemde ihtiyaç duyulan paket sayısı 1000 paketin altına düşmüştür.



Şekil 2.6. Olasılıksal Paket İşaretleme (Probabilistic Packet Marking)

PPM işleminin günümüz veri ağı yapısına uygulanması oldukça kolaydır ve bunun için yönlendirici cihazlarda ayrı bir donanıma ihtiyaç duyulmamaktadır. Firmaların bu yöntemin uygulanabilmesi için yönlendirici cihazlarına yazılım güncelleştirmesi yapmaları yeterlidir. PPM yönteminde iş yükü IP Geri İzleme yapacak olan hedef noktaya düşmektedir. Yönlendiriciler sadece gelen IP paketlerini işaretlerken hedef bilgisayarlar gelen çok sayıda paket üzerinde işlem

yapmak zorunda kalırlar. Hedef bilgisayarlar saldırı yollarını yeniden inşa etmeleri için çok miktarda hafızaya ihtiyaç duymaktalardır.

PPM ‘i temel alan yöntemler saldırı sırasında sadece saldırı paketlerinin geldiği noktaları belirleyebilmektedirler. DDoS saldırısı hayalet sunucular kullanılarak yapılmaktaysa sadece hayalet sunucular tespit edilebilmekte saldırıyı organize eden veya edenler bulunamaktadır.

2.5. IP Geri İzleme Yöntemlerinin Karşılaştırılması

IP Geri İzleme yöntemleri dört ana başlık altında toplanarak anlatılmıştır. Bu yöntemlerin karşılaştırılması Çizelge 2.1.’de gösterilmiştir.

Çizelge 2.1. IP Geri İzleme Yöntemlerinin Karşılaştırılması

IP Geri İzleme Yöntemi	Veri Ağı Yükü	Yönetim Yükü	Yönlendirici Yükü
Mesajlaşma	Düşük	Düşük	Düşük
Günlük Tutma	Düşük	Çok	Çok
Bağlantı Testi			
Giriş Hata Ayıklama	Düşük	Yüksek	Yüksek
Kontrollü Sel	Yüksek	Düşük	Düşük
Paket İşaretleme			
Rast Gele Olmayan Paket İşaretleme	Düşük	Düşük	Yüksek
Olasılıksal Paket İşaretleme	Düşük	Düşük	Düşük

Tüm yöntemler arasında var olan veri ağları yapısında kullanılması en kolay yöntem Olasılıksal Paket İşaretleme yöntemidir. Yönlendirici cihazlara ve veri ağına getirdiği düşük yük ve karmaşık olmayan yapısından dolayı PPM diğer yöntemlere göre daha kullanılabilir bir yöntemdir. Bu tezde önerilen IP Geri İzleme yöntemi PPM' i geliştirmeyi amaçlanarak geliştirilen bir yöntemdir.

3. OPNET (Optimized Network Engineering Tools)

Veri ağ yapılarının farklı durumlar altındaki tepkilerinin gözlenebilmesi ve ölçülebilmesi amacıyla simülasyon yazılımlarına ihtiyaç duyulmaktadır. Bu tür yazılımlar kullanılarak farklı ağ yapıları tasarlanılabilmekte ve ölçümler alınabilmektedir. Yazılımların sunduğu esnek yapılardan dolayı yeni geliştirilen algoritmalar veya protokoller tasarlanan ağ yapıları üzerinde gerçeklenebilmektedir. Piyasada bulunan başlıca veri ağları simülasyon yazılımları ise şunlardır: OPNET[2], NS2[3], QualNet[4], NetSim[5], OMNeT++[6]. Bu tezde gerek gelişmiş grafik kullanıcı ara yüzüne sahip olması, gerek C/C++ dilleri kullanılarak var olan yapılarda değişiklikler sağlaması ve elde edilen sonuçların güvenilir olmasından dolayı ve en önemlisi dünyada en çok tercih edilen ticari benzetim olması nedeniyle OPNET tercih edilmiştir.

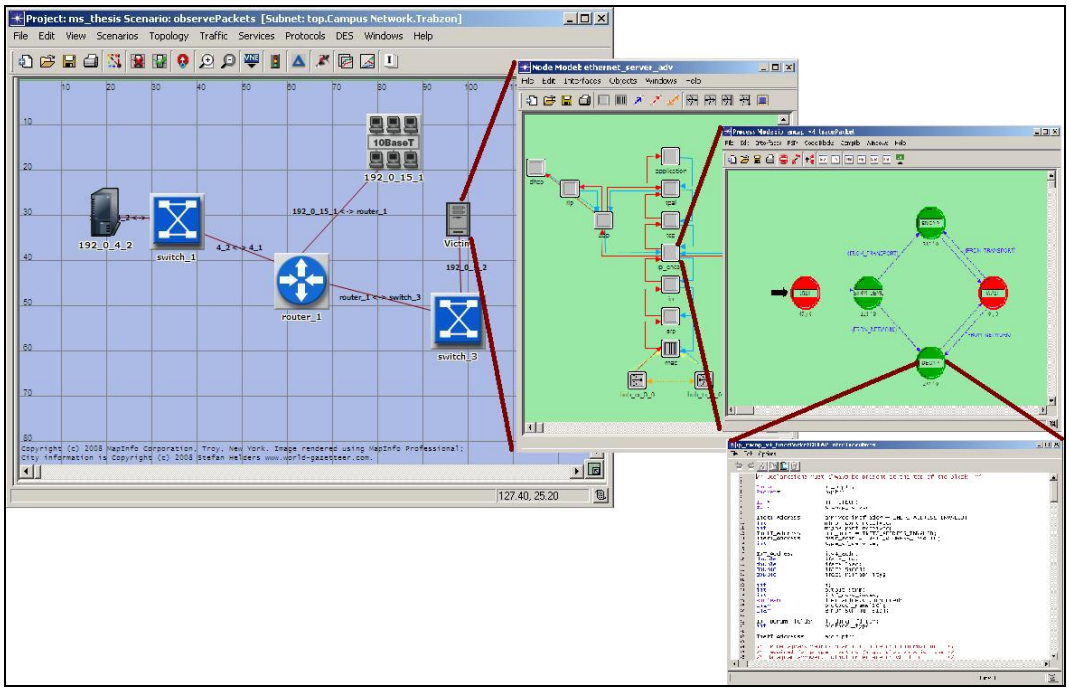
3.1. OPNET (Optimized Network Engineering Tools)

OPNET tüm veri ağı türlerini ve teknolojilerini destekleyen ve kullanımı en yaygın veri ağı simülasyon yazılımıdır. Simülasyonlardan alınan sonuçların geçerliliği üzerinde büyük bir güven vardır. OPNET, simülasyon sonuçların toplanması ve gösterilmesi kısımlarında güçlü bir performansa sahiptir. Ayrıca OPNET, veri ağlarının tasarımı için oldukça kullanışlı bir ara yüze sahiptir. Gerçek veri ağlarında yaygın biçimde kullanılan cihazların birçoğu OPNET'in veri ağı model kütüphanesinde sunulmaktadır. Kullanıcılar isterlerse bu cihaz modellerini kullanabilmekte veya değiştirebilmekte ya da kendi veri ağ cihazlarını tasarlayabilmektedirler. Esnek yapısı sayesinde eklentiler yapılarak cihazlara yeni özellikler de sağlanabilmektedir.

OPNET, Windows, Linux ve Solaris tabanlı işletim sistemlerinin üzerine kurulabilmektedir. OPNET yazılımında kullanılan modeller Şekil 3.1.'de gösterildiği gibi üç katmanlı hiyerarşik yapı üzerinde tasarlanmıştır [14]. Bu katmanlar sırasıyla şu şekildedir: Veri Ağı Modeli (Network Model), Düğüm

[2] http://www.opnet.com
[3] http://nsnam.isi.edu/nsnam/index.php/Main_Page
[4] http://www.qualnet.com
[5] http://www.tetcos.com
[6] http://www.omnetpp.org

Modeli (Node Model), İşlem Modeli (Process Model). Bu katmanlar iç içe tasarlanmıştır. Veri ağı modeli birden fazla düğüm modelinin bir araya gelmesi ile oluşmaktadır. Düğüm modeli ise içinde farklı işlem modellerinin bir araya gelmesiyle oluşmaktadır. Modellerin iç içe olması sayesinde alt model katmanında yapılan değişiklik o alt modeli kullanan tüm üst modellerin çalışmasını da değiştirmektedir. Veri ağı katman (Network Layer) yapısına benzeyen bu yapı sayesinde kullanıcılar her hangi bir katmanda yaptıkları değişiklik veya yeniliklerin tüm veri ağının davranışını nasıl değiştirdiğini gözlemleyebilmektedirler.



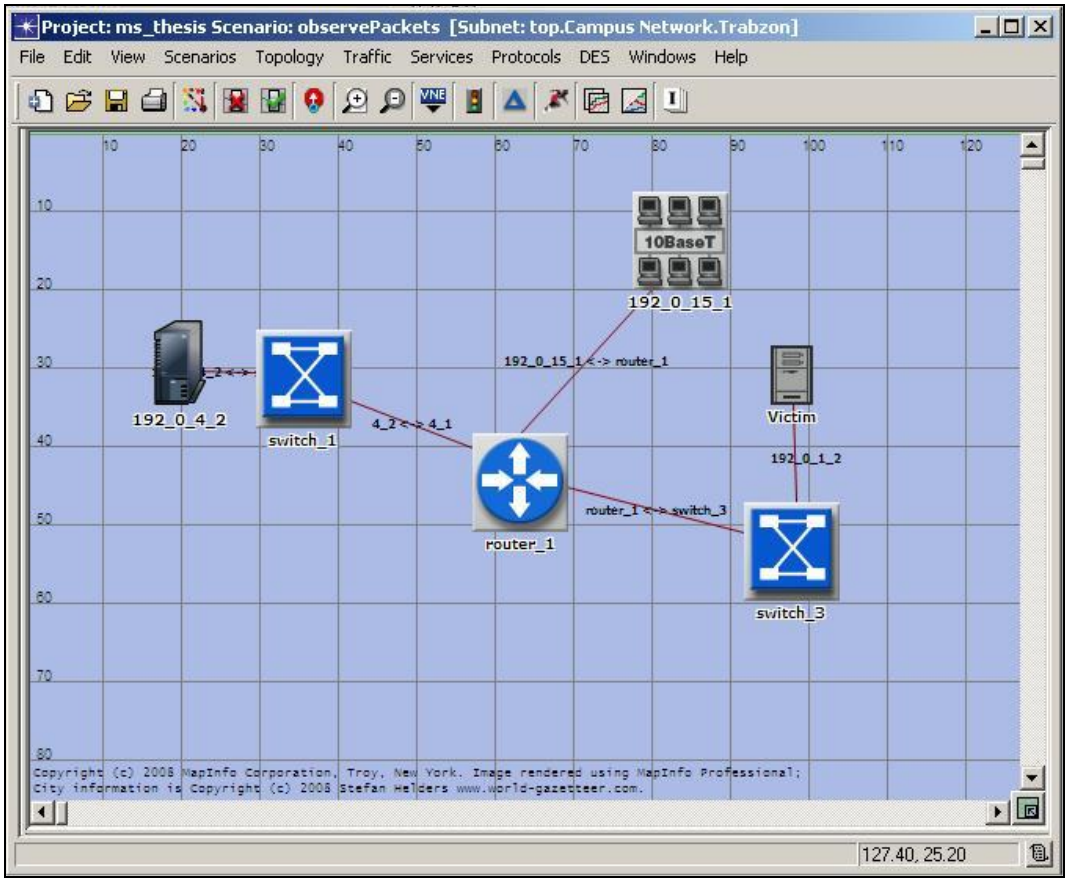
Şekil 3.1. OPNET Katmanlı Hiyerarşi

OPNET pek çok düzenleyiciden oluşmaktadır: Proje Düzenleyicisi (Project Editor), Düğüm Düzenleyicisi (Node Editor), İşlem Düzenleyicisi (Process Editor), Bağlantı Model Düzenleyicisi (Link Editor), Paket Biçim Düzenleyicisi (Packet Format Editor).

3.1.1. Proje Düzenleyicisi (Project Editor)

Proje düzenleyicisi, veri ağlarının tasarlandığı ana kısımdır. Bu kısımda standart model kütüphanelerinin olduğu paletler kullanılarak veri ağı topolojisi

tasarlanmaktadır. Veri ağında hangi değerlerin ölçüleceği proje düzenleyici kısmında belirlenmektedir. Simülasyonlar buradan çalıştırılmakta ve sonuçları buradan gözlenebilmektedir.



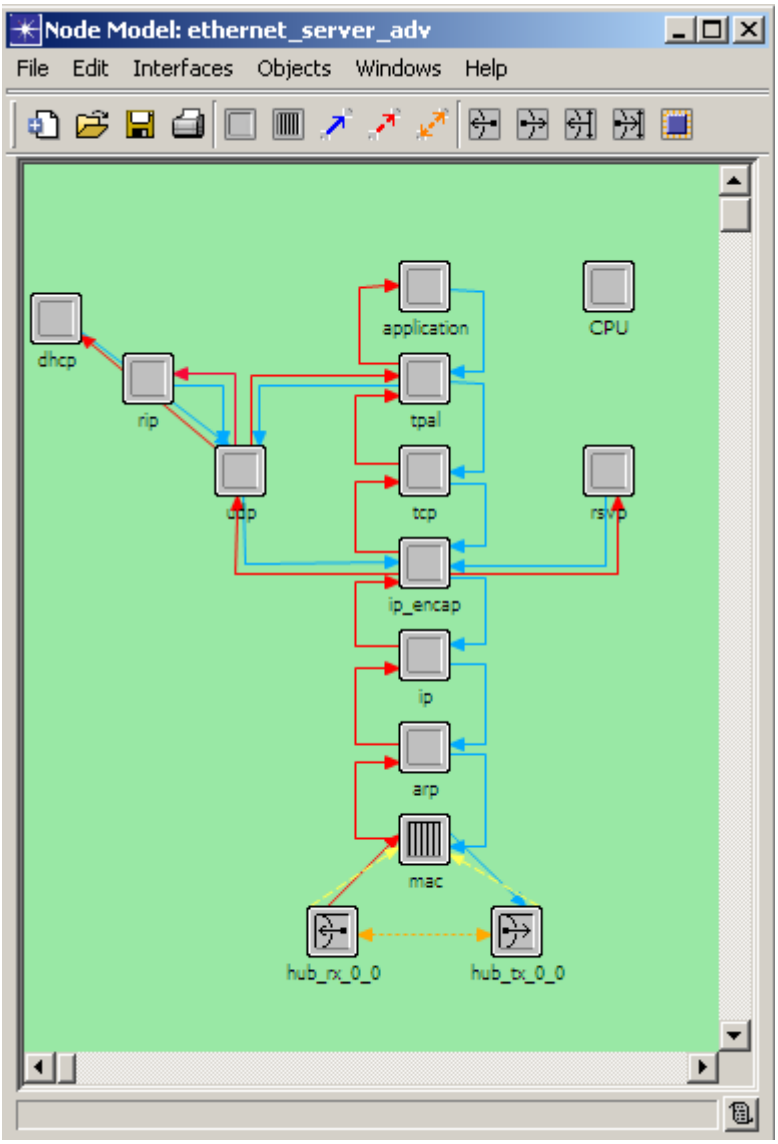
Şekil 3.2. Proje Düzenleyicisi

Tasarlanan farklı veri ağ yapıları alt-ağlar (subnetler) altında toplanabilmektedir. Subnetler birbirlerine bağlanarak farklı veri ağ yapılarının bir arada çalışmaları da incelenebilmektedir. Proje düzenleyicinin kullanıcılarına sunduğu model kütüphaneleri çok zengindir. Pek çok firmaya ait veri ağ cihazını burada bulmak mümkündür. Ayrıca proje düzenleyici, sunduğu modeller üzerinde konfigurasyon değişiklikleri yapılmasına da olanak sağlamaktadır.

3.1.2. Düğüm Düzenleyicisi (Node Editor)

Düğüm düzenleyicisi kullanılarak veri ağı modellerini oluşturan düğüm modelleri düzenlenebilmektedir. Düğümler modüler yapıda tasarlanmıştır. Bu sayede farklı düğüm modelleri paket akışları ve statik kablolarla Şekil 3.3.'te

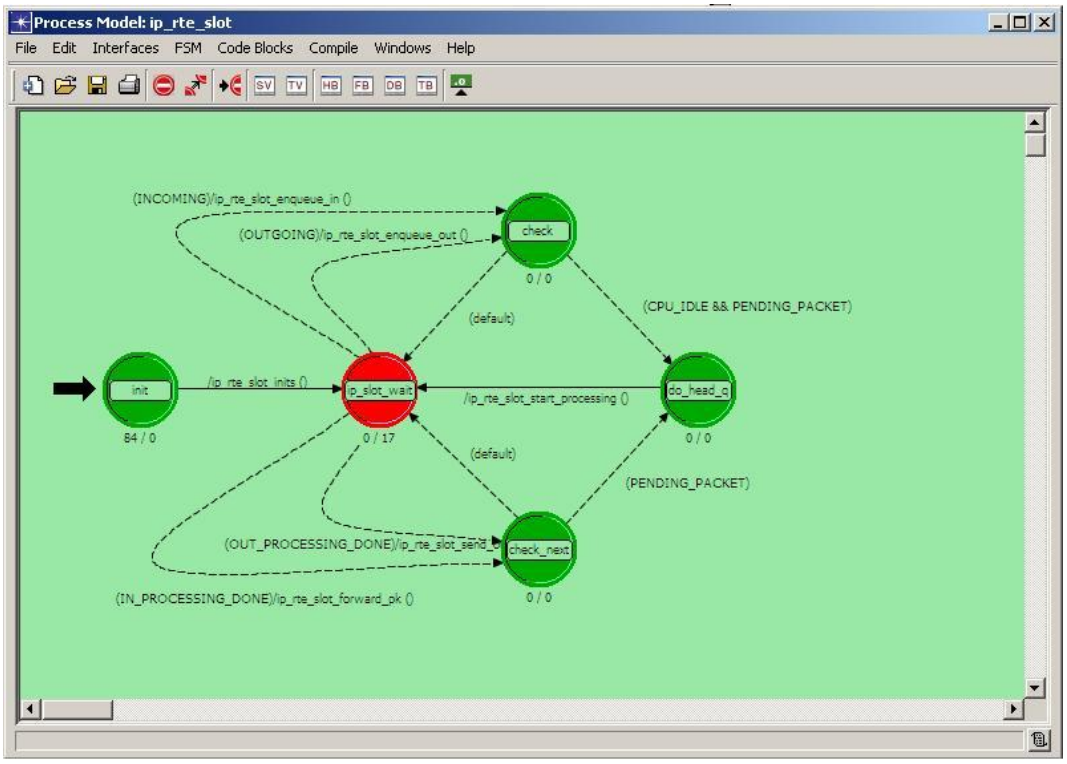
gösterildiği gibi bağlanabilmekte ve bir arada çalışabilmektedirler. Düğüm modelleri arasındaki bağlantılar kullanılarak paket ve durum bilgilerinin kendi aralarında paylaşımı da sağlanabilmektedir. Her düğüm modellinin paket üretme, paket bekletme, paket işleme, paket alma veya gönderme gibi farklı görevleri vardır.



Şekil 3.3. Düğüm Düzenleyicisi

3.1.3. İşlem Düzenleyicisi (Process Editor)

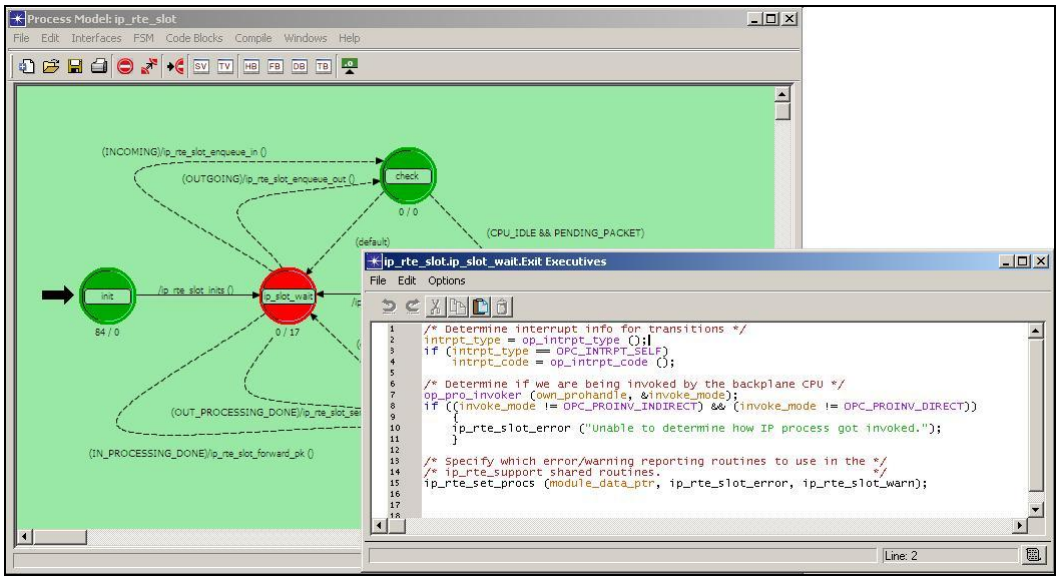
Düğüm düzenleyici tarafından yaratılan düğüm modellerinin nasıl çalışacaklarının kontrol edildiği kısım İşlem düzenleyicisidir. İşlem modelleri Şekil 3.4.'te gösterildiği gibi sonlu durum makinelerinden (Finite State Machine, FSM) oluşmaktadır.



Şekil 3.4. İşlem Düzenleyicisi

Şekil 3.4.'te gösterilen ikonalar FSM durumlarını, aralarındaki çizgiler ise bu durumlar arasındaki geçişleri belirtmektedir. FSM durumlarındaki ve durumlar arasındaki geçişlerdeki tüm işlemler C / C++ kodları ile yapılmaktadır. Bu kodlara İşlem Düzenleyicinin araç çubuğunda bulunan tuşlarla ulaşılmaktadır. FSM durumlarını sembolize eden ikonaların üst kısımlarına tıklandığında duruma girildiğinde, alt kısımlarına tıklandığında ise durumdan çıkıldığında çalıştırılacak C/C++ kodları görüntülenmektedir (Şekil 3.5.). Bu kodlar üzerinde değişiklikler veya eklentiler yapılarak veri ağı çalışma yapısı değiştirilebilmektedir. Bu

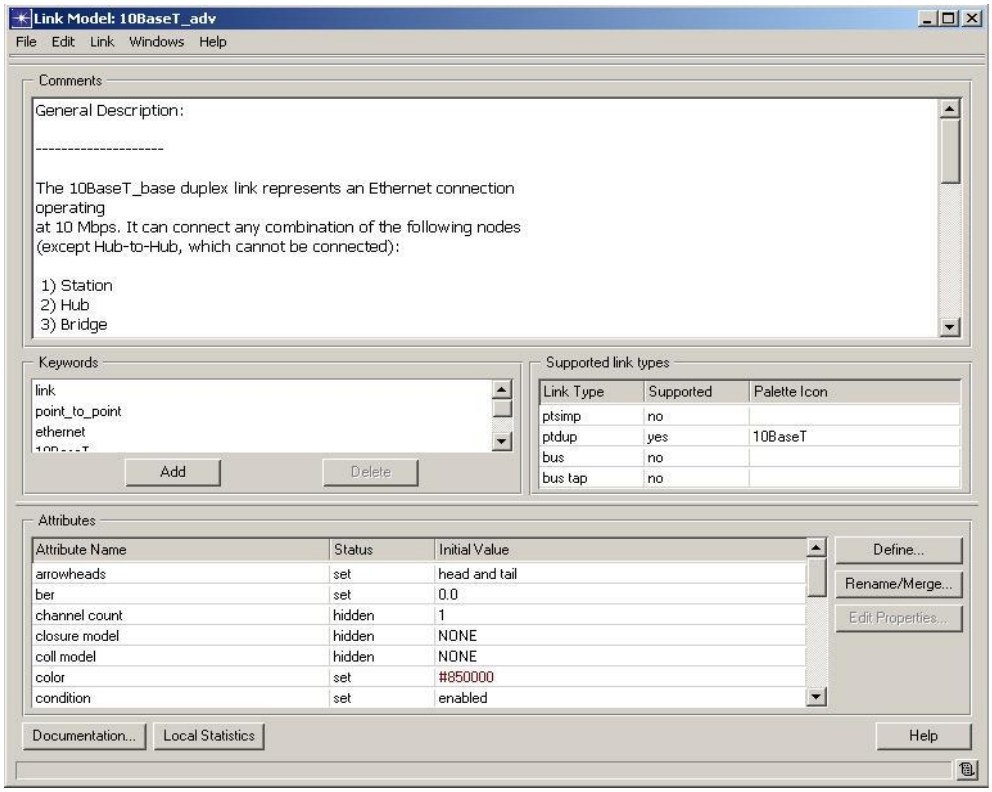
esneklik OPNET üzerinde farklı algoritmaların gerçeklenmesine olanak sağlamaktadır.



Şekil 3.5. FSM Durum Çıkış Kodları

3.1.4. Bağlantı Model Düzenleyicisi (Link Model Editor)

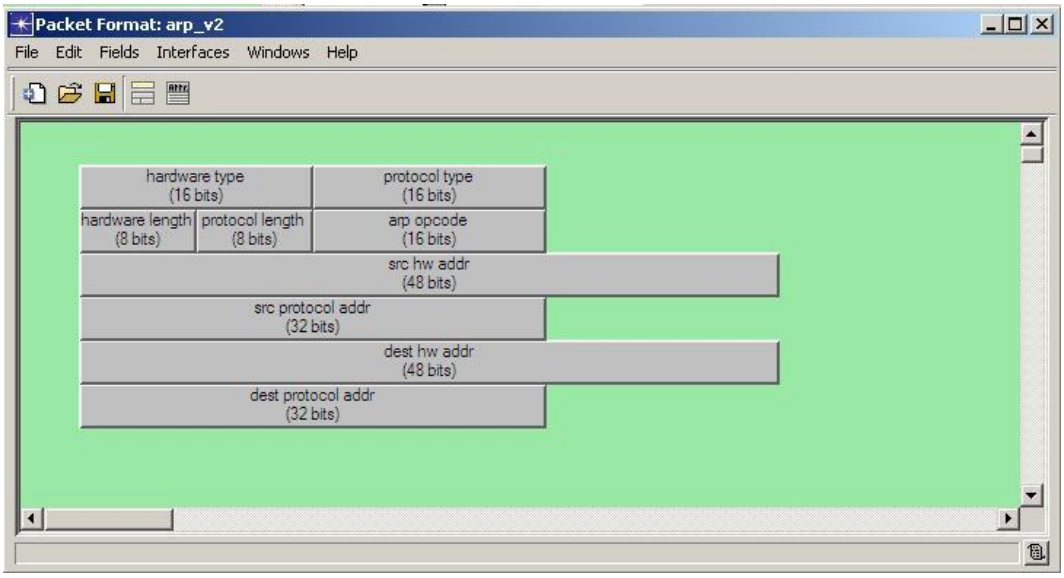
Bağlantı model düzenleyici (Şekil 3.6.) farklı yapıda bağlantı nesneleri yaratılmasına olanak sağlamaktadır. Bu sayede OPNET ile yaratılan veri ağları topolojilerinde farklı yapıda bağlantılar kullanabilmektedir. Bağlantı model düzenleyicisi kullanılarak tasarlanan her bağlantının ayrı özelliği ve gösterimi olabilmektedir.



Şekil 3.6. Bağlantı Model Düzenleyici

3.1.5. Paket Biçim Düzenleyicisi (Packet Format Editor)

Paket biçim düzenleyicisi (Şekil 3.7.) ile bir paketin içyapısı alanlar kullanılarak düzenlenebilmektedir. Paket yapıları bir veya birden fazla alandan oluşmaktadır. Paket biçim düzenleyicisi kullanılarak paket biçimine yeni alanlar eklenebilmekte veya var olan alanlar değiştirilebilmektedir. Paket biçiminde gösterilen kısımların alanları, alanların bit sayısı ile doğru orantılıdır.



Şekil 3.7. Paket Biçim Düzenleyicisi

4. DİNAMİK DEĞİŞEN PAKET İŞARETLEME OLASILIĞI YÖNTEMİ

Bu tezde Olasılıksal Paket İşaretlemeye üzerine kurulmuş bir paket işaretleme yöntemi önerilmektedir. Olasılıksal Paket İşaretleme yönteminde yönlendiriciye gelen tüm IP paketleri sabit bir olasılıkla işaretlenmektedir. Önerilen yöntemde ise yönlendirici üzerinden geçen paket trafiği gözlemlenerek, trafik yoğunluğuyla doğru orantılı giriş noktalarındaki paket işaretleme olasılıkları değiştirilmektedir. Bu sayede, (D)DoS saldırılarında IP paket trafiği artacağından işaretlenen saldırı paketlerinin normal paketlere oranı, literatürde önerilen istatistiksel oranlardan daha fazla olmaktadır. Paket işaretleme olasılıkları dinamik olarak değiştiğinden önerilen yönteme "Dinamik Değişen Paket İşaretleme Olasılığı Yöntemi" adı verilmiştir.

Literatürde önerilen olasılıksal paket işaretleme yöntemleri kullanıldığında, yönlendiriciler gelen tüm IP paketlerini sabit bir olasılıkla işaretlemektedirler. Bu tezde önerilen yöntemde ise, IP paketlerinin yönlendiricilere girdikleri ve çıktıkları noktaların trafik yoğunluğuna bakılarak buradaki paket işaretleme olasılıkları trafik yoğunluğuyla doğru orantılı değiştirilmektedir. (D)DoS saldırılarında paket trafiği artacağı göz önünde bulundurulduğunda hiç şüphesiz işaretlenmiş saldırı paketi sayısı normal paket sayısına göre daha fazla olacaktır. Bu tezde önerilen yöntem kullanıldığında, saldırıların yönlendiricilere girdikleri ve çıktıkları noktalarının paket işaretleme olasılıkları artacağından işaretlenmiş saldırı paketlerinin normal paketlere oranı literatürde önerilen yöntemlere göre daha fazla olacaktır. Saldırı esnasında normal trafikle gelen paketlerin işaretlenme olasılığı azalacağından işaretlenen normal paket sayısı da azalacaktır. Böylelikle amaçlanan, saldırı noktalarının belirlenmesi için gerekli toplam işaretlenmiş paket sayısı aynı kalmakla birlikte yönlendiriciler daha az paket işaretlemekte ve yönlendiricilerin yükünün azaltılmasıdır.

(D)DoS saldırıları Bölüm 2'de de bahsedildiği gibi birden fazla saldırı noktasından farklı veri ağı yolları kullanılarak yapılmaktadır. Bu farklı yolları ayırt etmek için sadece IP adresleri yeterli olmamaktadır. Bunun için paketlere yönlendiricilerin birbirleriyle olan görece uzaklık bilgilerinin de eklenmesi gerekmektedir. Bu bilgi, her paket, yönlendirici değiştiğinde değişikliği belirtecek bir işaret olmalıdır ve bunun için en kolay yöntem de zıplama sayısıdır. Önerilen

yöntemde her yönlendiricin kendisine özel bir başlangıç zıplama sayısı vardır. Yönlendiriciler zıplama sayılarını belli periyotlarda değiştirmektedirler. Bu sayede işaretlerden elde edilecek yönlendirici sıralamasını bozmak için zıplama sayısını değiştirmek isteyen kişi veya kişiler engellenmektedir. Eğer yönlendiriciye gelen paket hiç işaretlenmemişse yönlendirici, yönlendiriciye ait tekil (unique) zıplama sayısını paket işaretine eklemektedir. Eğer paket daha önce işaretlenmişse, yönlendirici daha önce eklenen zıplama sayısını bir arttırmakta ve paket işaretine eklemektedir. Bu sayede saldırılardan etkilenen hedef bilgisayar, gelen paketleri incelediğinde işaretler içindeki zıplama sayılarını kullanarak işaretlerden elde edilen IP adresleri arasında sıralama yapabilmekte ve saldırı yollarını belirleyebilmektedir. Yöntemin pseudo kodları Şekil 4.1., Şekil 4.2., Şekil 4.3. ve Şekil 4.4.'te gösterilmektedir.

```
Prosedür paket_işaretle
Yönlendirici R, yönlendiriciye gelen IP paketi p, IP paketlerinin yönlendiriciye
girdiği ara birim adresi I, IP paketlerinin yönlendiriciden çıktığı ara birim adresi
E, İki farklı arabirim arasındaki yol Yol( . , . )
R' ye I noktasından girip E noktasından çıkan her paket için
 Yol(I,E).paket_sayısı++
 Olasılıkları_Tekrar_Hesapla prosedürünü çağır
 [0,1) arasında rast gele bir sayı üret ve üretilen_sayı'ya ata
  Eğer üretilen_sayı <= Yol(I,E).olasılık ise
        Eğer p.Ayrılmış_Bayrak == '0' ise
                p.Ayrılmış_Bayrak = 1
                p.Opsiyonlar ='00000001' + R.Tekil_Zıplama_Sayısı + I
        Değilse
                Zıplama_Sayısı = p.Opsiyonlar[8,31]
                Zıplama_Sayısı++;
                p.Opsiyonlar = "00000001" + Zıplama_Sayısı + I
Prosedür Bitir
```

Şekil 4.1. Paket İşaretleme İşlemi

Prosedür Olasılıkları_Tekrar_Hesapla

Yönlendirici R, yönlendiricinin ara yüz adres sayısı N, paketlerin yönlendirici üzerinden geçebilecekleri yol Yol[.], yönlendiricinin PPM yönteminde önerilen paket işaretleme olasılığı pr

```
Toplam_Gelen_Paket_Sayısı=0
i  0'dan (N*(N-1))'e kadar
        Toplam_Gelen_Paket_Sayısı += Yol[i].paket_sayısı

i  0'dan (N*(N-1))'e kadar
    Yol[i].olasılık=(Yol[i].paket_sayısı / Toplam_Gelen_Paket_Sayısı) * pr
```

Prosedür Bitir

Şekil 4.2. Paket İşaretleme Olasılıkların Hesaplanması İşlemi

Prosedür İşaretleri_Sakla

Gelen IP paket p, paketlerdeki işaret M, paketlerdeki işaretlerin tutulduğu tablo T

```
    Gelen Tüm Paketler için
        Eğer p.Ayrılmış_Bayrak == '1' ise
            M.IP_Adres = p.Opsiyonlar[32,63]
            M.Zıplama_Sayısı = p.Opsiyonlar[8,31]
            M'yi T'ye ekle
```

Prosedür Bitir

Şekil 4.3. İşaretlenmiş Paketlerin Saklanması İşlemi

Prosedür Geri_İzleme_Yap

Paketlerdeki işaretlerin tutulduğu tablo T, T tablosunda saklanan işaretlerden herhangi biri M, Geri İzleme Tablosu G, Zıplama Sayısı Z

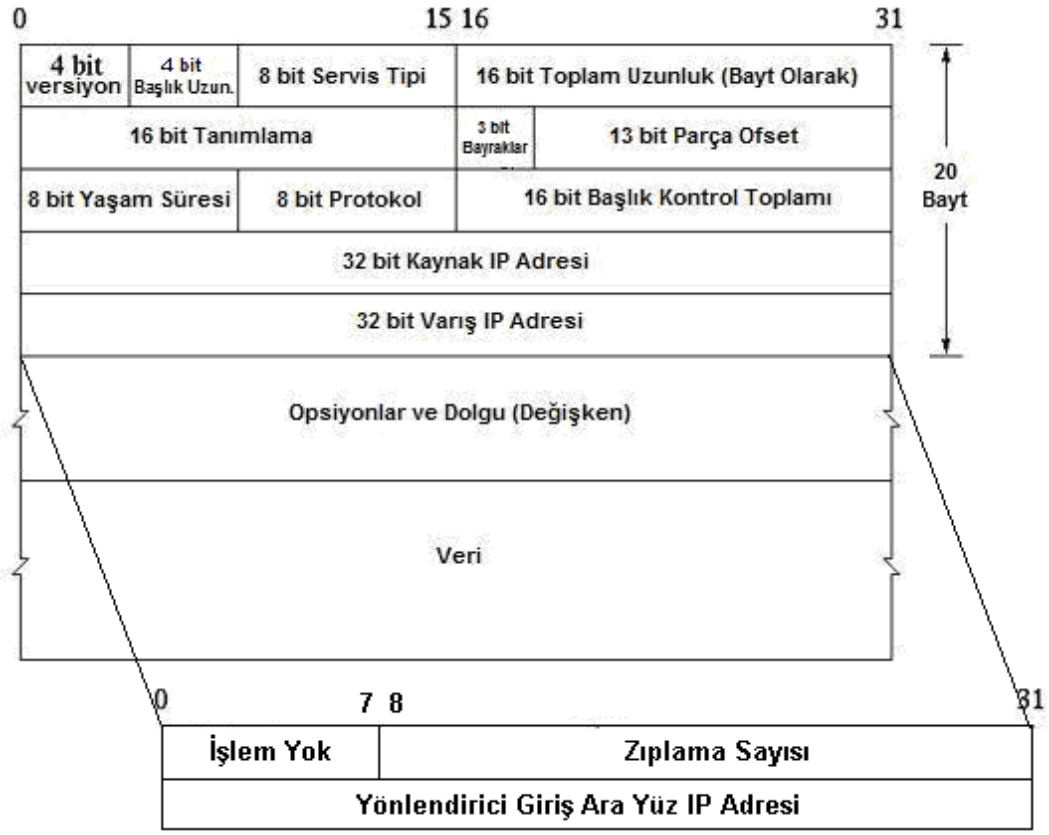
```
Döngü1:     Eğer T tablosu boş değilse
            T içindeki en büyük M.Zıplama_Sayısı'nı bul ve Z'ye ata
            Döngü2:     T içinde Z değerine sahip M'leri bul
                  Eğer M'ler T'de var ise
                        M'leri T'den çıkar ve G'ye ekle
                        Z--
                        Döngü2'ye git
                  değilse
                        G'teki M değerlerini kullanarak yolu belirle
                        Döngü1'e git
```

Prosedür Bitir

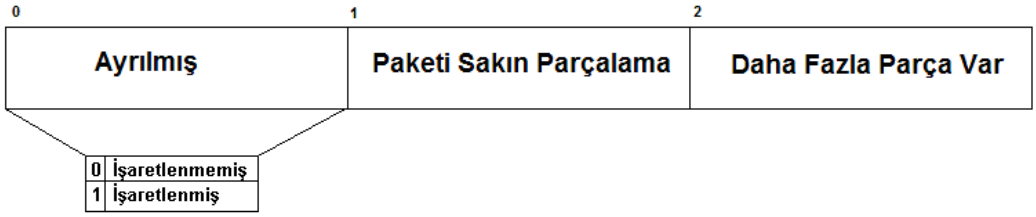
Şekil 4.4. Geri İzleme İşlemi

Paket işareti 32-bitlik yönlendirici giriş ara birim adresi ve 24-bitlik zıplama sayısından oluşmaktadır (Şekil 4.5.). Paketler işaretlenirken IP Datagram'da bulunan *opsiyonlar ve dolgu* (options and padding) kısmıyla *ayrılmış bayrak* (reserved flag) (Şekil 4.6.) biti kullanılmıştır. Yönlendiriciler paketleri işaretlendiklerinde ayrılmış bayrağın değerini "1" olarak değiştirmektedirler. Paketin yönlendiriciye girdiği ara yüz adresi ile zıplama sayısı, paketin *opsiyonlar ve dolgu* kısmına eklenmektedir. Eklenen bilgilerin diğer opsiyonlarla karışmaması için bilgilerin önüne *işlem yok* (no operation) [12] etiketi eklenir. 8-bit uzunluğundaki *işlem yok* etiketini kullanmak için paket işaretinin başına "00000001" değeri eklenmektedir. Pakete eklenen işaretin IP Datagram'a getirdiği yük toplam 64 bit'tir. Bu tezde önerilen paket işaretleme yöntemi daha öncede bahsedildiği gibi saldırı noktalarını belirlemek için daha az işaretlenmiş pakete ihtiyaç duyduğundan 64-bit'lik yük genel ağ trafiği içerisinde getireceği yük azımsanacak ölçüde olmaktadır. İşaret eklendikten sonra paketin

yapısı değiştiğinden *başlık uzunluk* (header length), *toplam uzunluk* (total length) ve *başlık kontrol toplamı* (header checksum) kısımları güncellenmektedir.



Şekil 4.5. İşaretlenen IP Datagram Yapısı

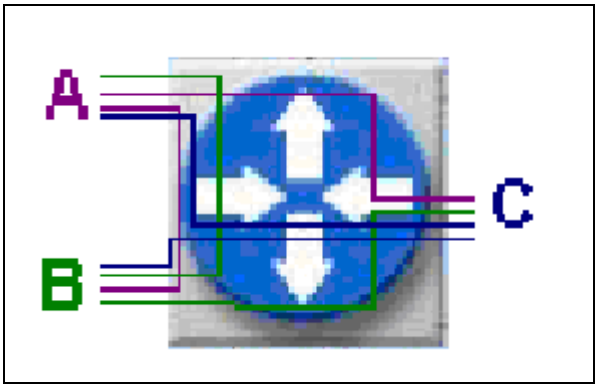


Şekil 4.6. İşaretlenen Bayraklar (Flags) Yapısı

4.1. Dinamik Paket İşaretleme Olasılığının Mantığı

Yönlendiriciye gelen IP paketlerinin giriş ve çıkış ara yüzleri belirlendikten sonra yönlendirici üzerindeki paket yolları da bunlara bağlı olarak belirlenebilmektedir (Şekil 4.7.). Önerilen yöntemde paket yollarından geçen her paket için o paket yolundan geçen paket sayısı bir arttırılacaktır. Olasılıksal paket

işaretleme yönteminde önerilen yönlendiriciye gelen herhangi bir IP paketinin işaretlenme olasılığı p olarak kabul edilmektedir. Bu tezde önerilen yöntemdeki paket işaretleme olasılığı ise Şekil 4.2.'de gösterildiği gibi hesaplanmaktadır. Bu sayede p olasılığı paket yollarındaki trafik yoğunluğuna göre dağıtılmaktadır. Böylece trafiğin yoğunluğunun çok olduğu paket yollarının paket işaretleme olasılığı trafiğin az olduğu paket yollarına göre daha büyük olacaktır. (D)DoS saldırılarının kullandığı paket yollarındaki trafik yoğunluğu artacağından işaretlenen saldırı paketlerinin normal paketlere oranı da artmış olacaktır. Bu sayede yönlendiriciler aynı sayıda paket işaretleseler de saldırı trafiğini belirleyecek paket sayısı daha fazla olacaktır. Böylece, önerilen yöntemle yönlendiricilerin paket işaretleme işlem yükü azaltılacak, ayrıca ağ üzerinde daha az işaretlenmiş paket sayısı da bant genişliği kullanılırlığı açısından avantaj sağlayacaktır.



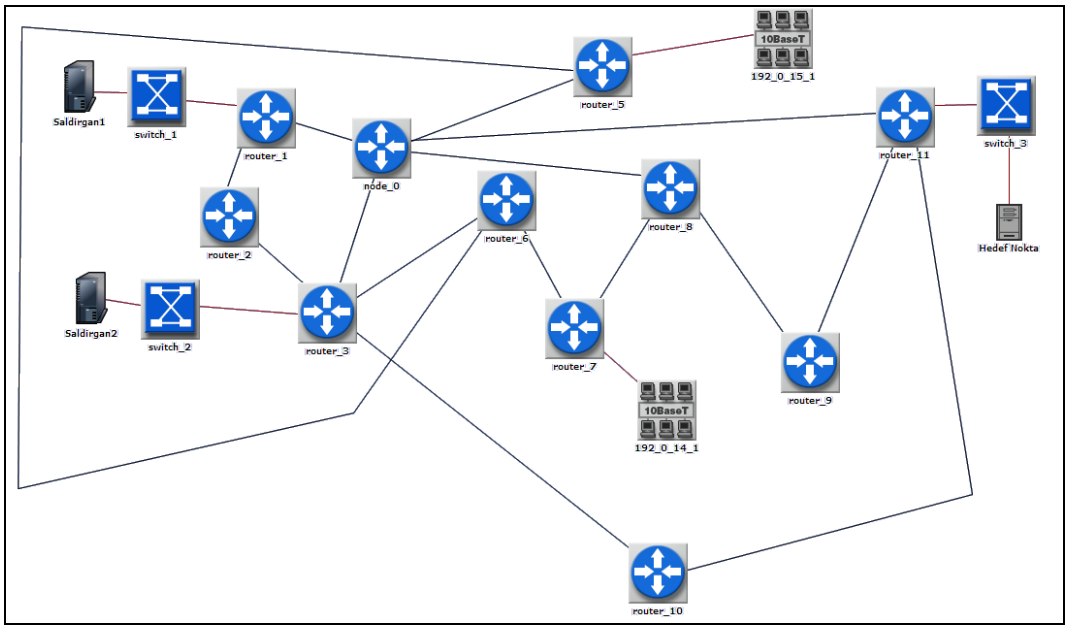
Şekil 4.7. Yönlendirici Üzerindeki Paket Yolları

4.2. Yöntem Benzetimi

Öncelikle bu tezde önerilen yöntem, matematiksel olarak analiz edilmiş ve belirgin bir iyileştirme saptanmıştır. Ancak hiç şüphesiz yöntemin gerçek bir ağ üzerindeki etkilerinin izlenmesi, yöntemin niteliğinin belirlenmesi açısından oldukça önemlidir. Bu yöntemin gerçek bir ağ altyapısına uyarlanması için yönlendiricilerde yazılımsal bir güncelleme yapılması gerektiğinden, sistemin bire bir benzetiminin yapılması gerekmektedir.

Önerilen yöntemin benzetiminin yapılması için Şekil 4.8.'teki veri ağı topolojisi OPNET'te oluşturulmuştur. Tezde sunulan paket işaretleme algoritması

yönlendiricilerin *IP İşlem Bilgisi* (IP Processing Information) kısmında *İşleme Planı* (Processing Scheme) bölümüne eklenerek gerçeklenmiştir. Ayrıca saldırı yapacak bilgisayarlara saldırı trafiği üretebilecek trafik profilleri tanımlanmıştır. Saldırıların hedefi olan bilgisayarın "ip_encap" adlı düğüm modelinin "DECAP" adlı sonlu durum makinesine, bu bilgisayara gelen paketleri inceleyen, işaretlenmiş paketlerden işaret bilgilerini çıkartıp saklayabilen ve işleyebilen geri izleme algoritması eklenmiştir.

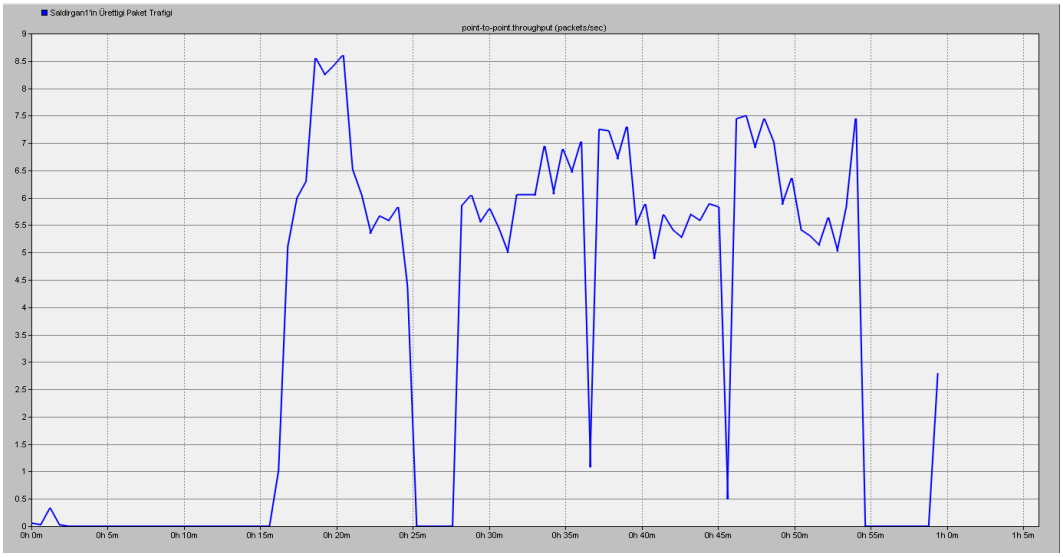


Şekil 4.8. Deneylerde kullanılan Veri Ağı Topolojisi

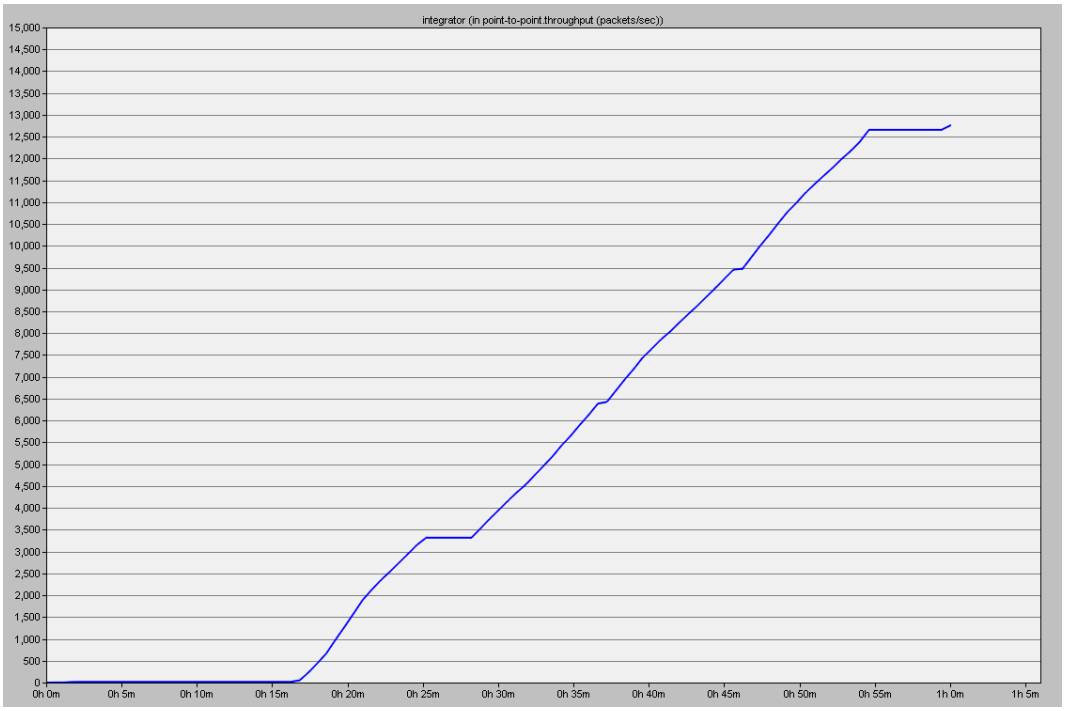
4.3. Deneyler

Dinamik Değişen Paket İşaretleme Olasılığı yönteminin sınanması için Şekil 4.8.'teki veri ağı topolojisi oluşturulmuştur. Oluşturulan veri ağı topolojisinde iki farklı yöntem uygulanarak deneyler yapılmıştır. Bu yöntemlerden bir tanesi literatürde önerilen olasılıksal paket işaretleme yöntemi bir diğeri ise bu tezde önerilen Dinamik Değişen Paket İşaretleme Olasılığı yöntemidir. Deneyler sırasında kullanılan değerler ve trafik yapıları gösterilmiştir:

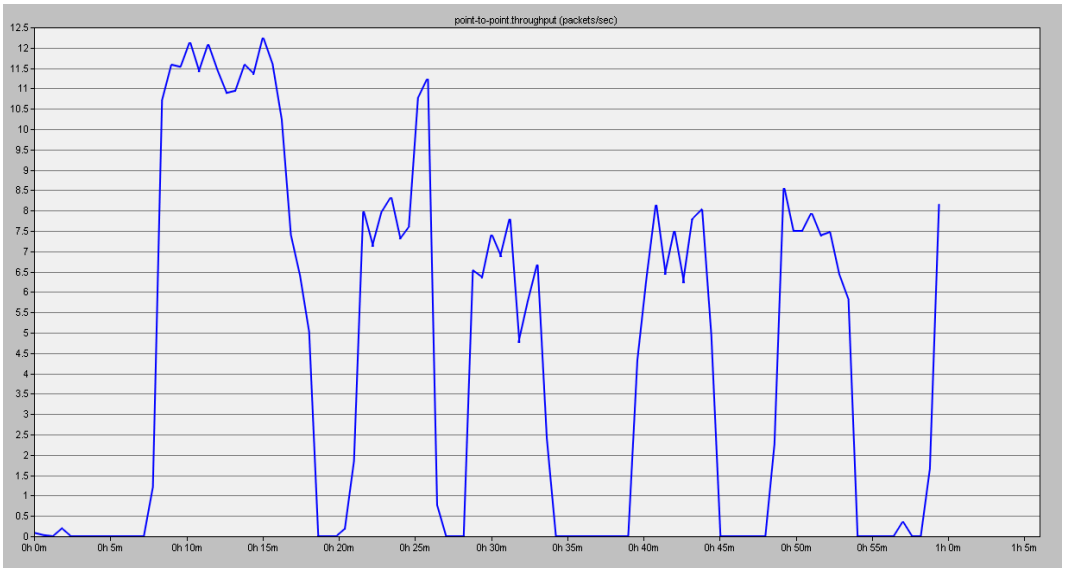
Saldırı kaynağı sayısı	:	2
LAN sayısı	:	2
LAN'lara bağlı kullanıcı sayısı	:	50
Toplam yönlendirici sayısı	:	11
Saldırı hedef sayısı	:	1
Simülasyon süresi	:	3600 saniye
Saldırı kaynak noktalarının IP Adresleri	:	192.0.4.2, 192.0.13.1
LAN'ların IP Adresleri	:	192.0.14.1, 192.0.15.1



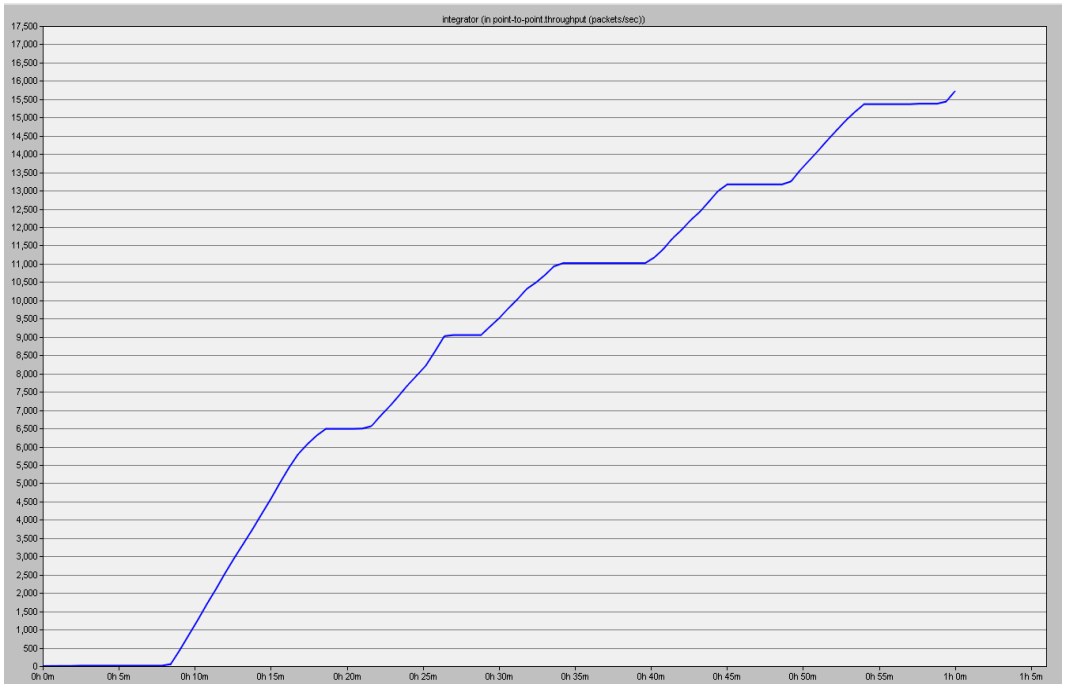
Şekil 4.9. 192.0.4.2 IP'li Saldırganın Ürettiği Trafik (paket/saniye)



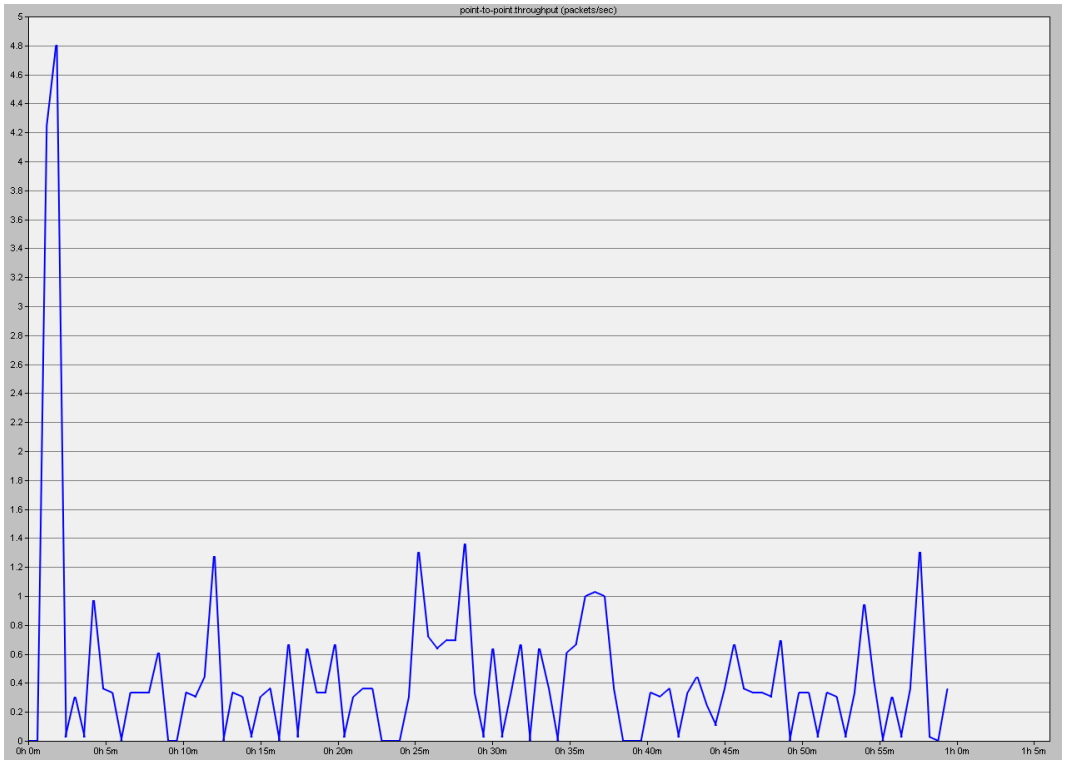
Şekil 4.10. 192.0.4.2 IP'li Saldırganın Ürettiği Toplam Paket Sayısı



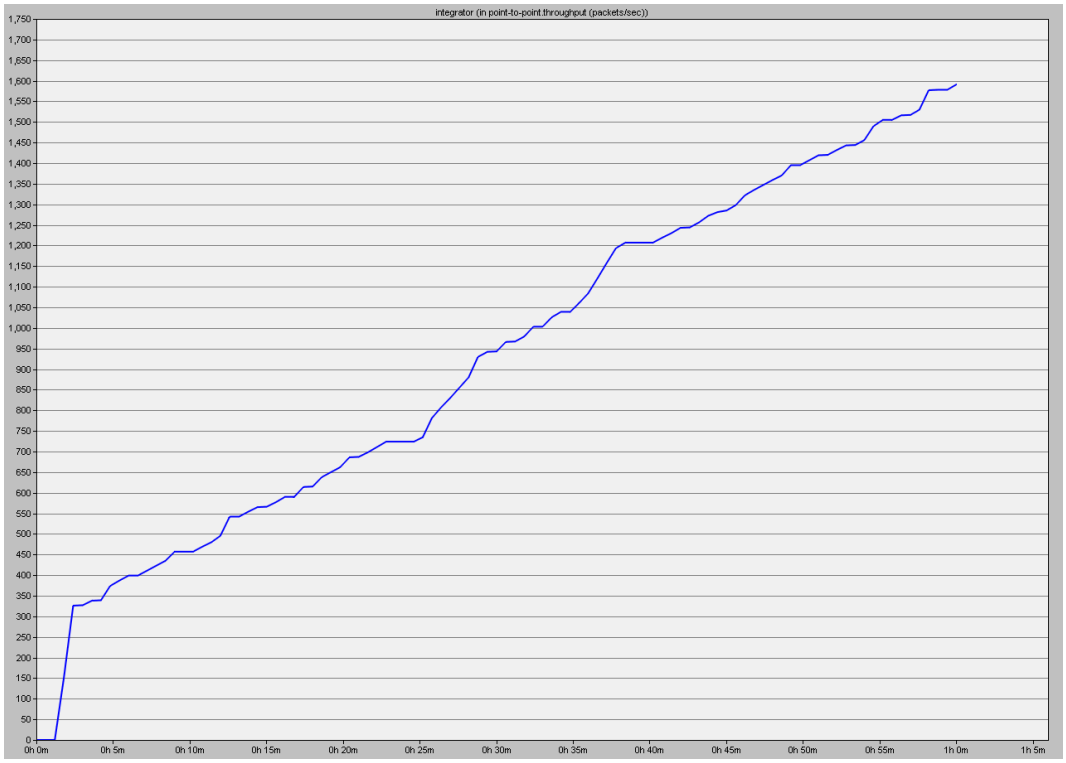
Şekil 4.11. 192.0.13.1 IP'li Saldırganın Ürettiği Trafik (paket/saniye)



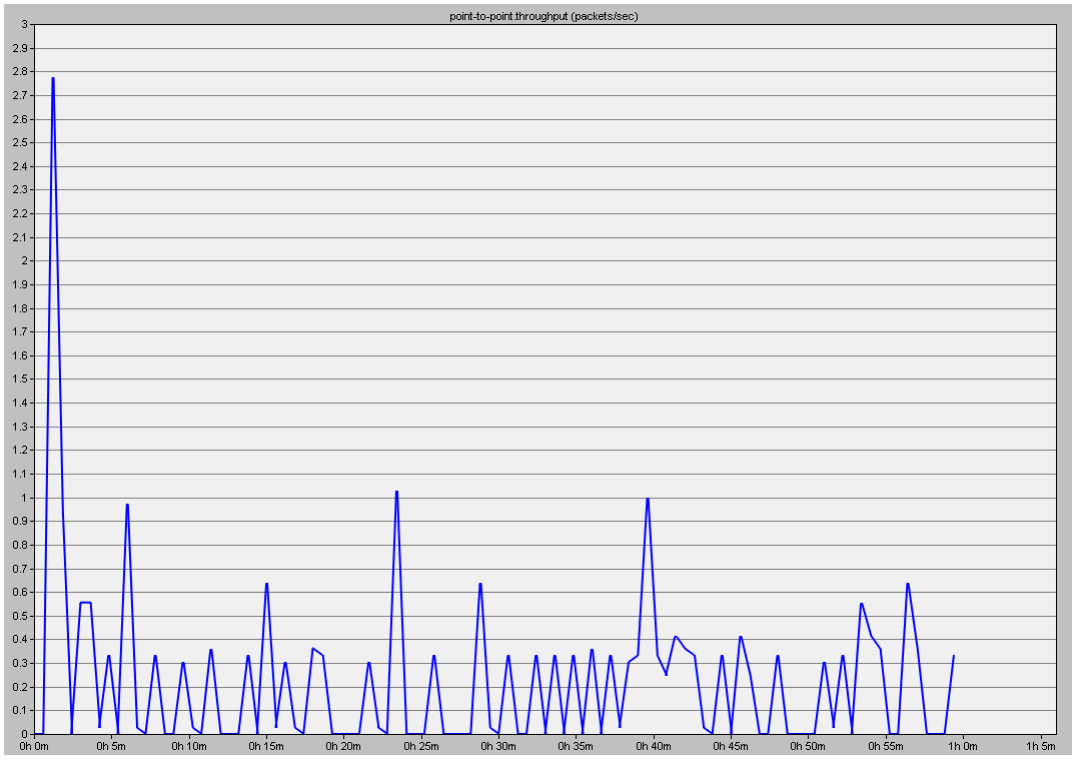
Şekil 4.12. 192.0.13.1 IP'li Saldırganın Ürettiği Toplam Paket Sayısı



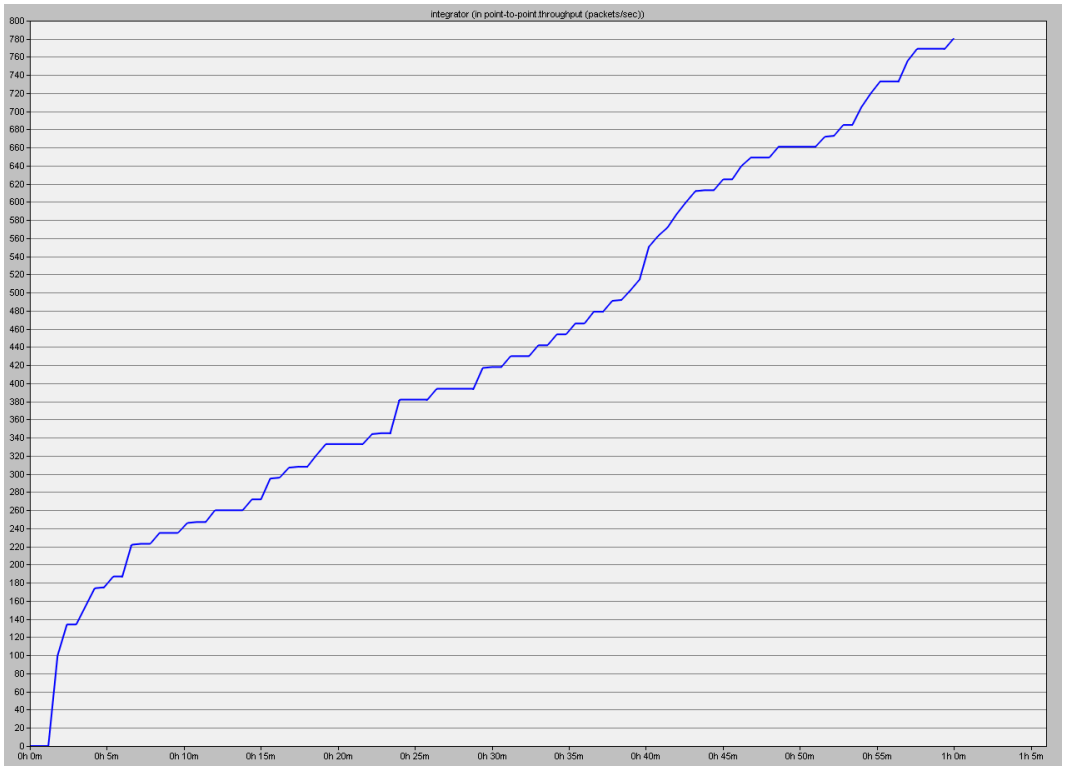
Şekil 4.13. 192.0.14.1 IP'li LAN'ın Ürettiği Trafik (paket/saniye)



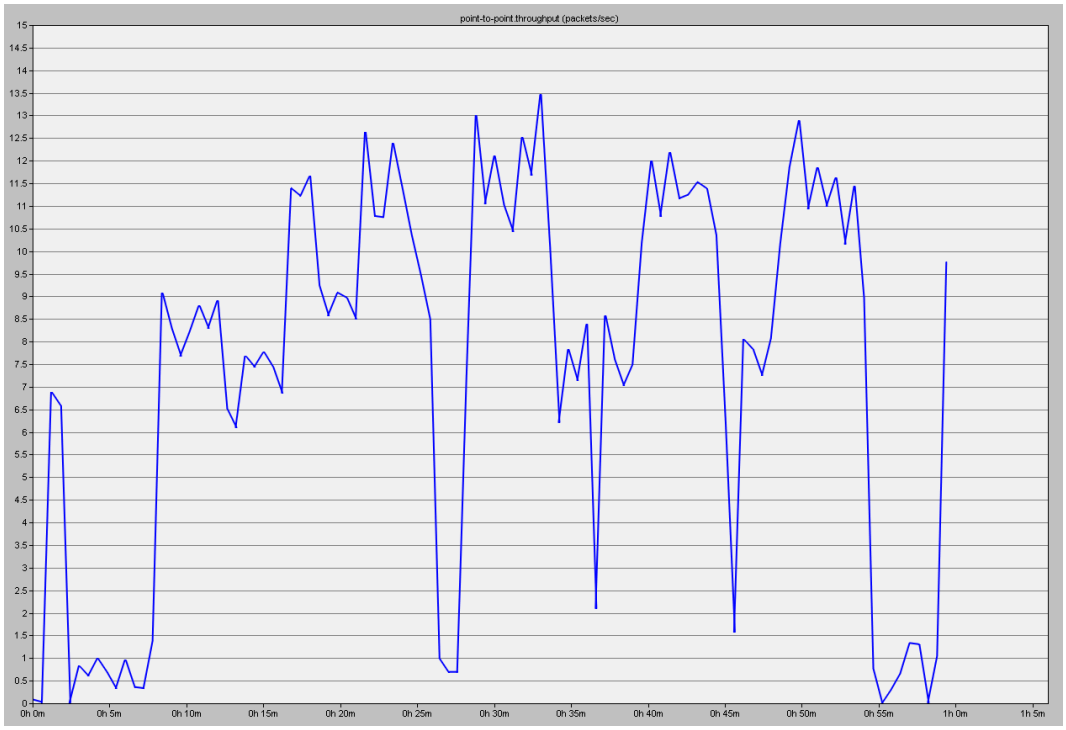
Şekil 4.14. 192.0.14.1 IP'li LAN'ın Ürettiği Toplam Paket Sayısı



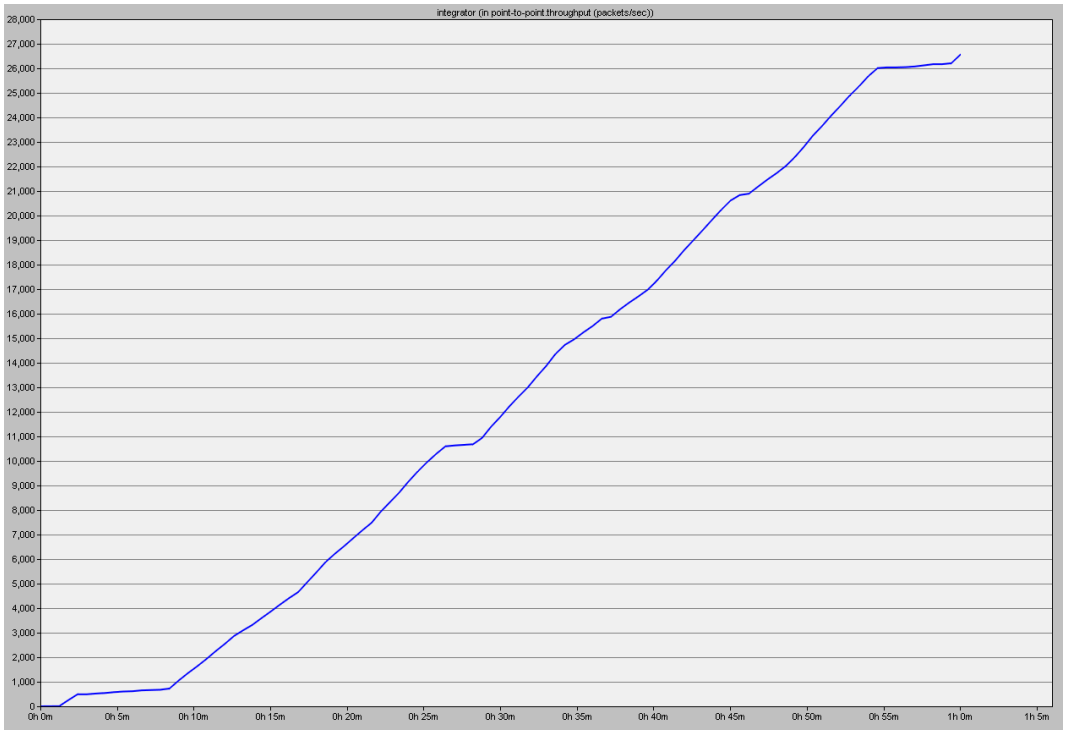
Şekil 4.15. 192.0.15.1 IP'li LAN'ın Ürettiği Trafik (paket/saniye)



Şekil 4.16. 192.0.15.1 IP'li LAN'ın Ürettiği Toplam Paket Sayısı



Şekil 4.17. 192.0.13.1 IP'li Hedef Noktaya Gelen Trafik (paket/saniye)



Şekil 4.18. 192.0.13.1 IP'li Hedef Noktaya Gelen Toplam Paket Sayısı

Deney 1: Bu deneyde, literatürde önerilen olasılıksal paket işaretleme yöntemi kullanılarak benzetim yapılmıştır. Herhangi bir paketin yönlendirici tarafından işaretlenme olasılığı 0.05 seçilmiştir. Simülasyon 3600 saniye sürmüştür. Paketlerin hangi kaynaktan çıktığı, işaretlendikleri yönlendiricilerin hangi giriş ve çıkış noktalarını kullandıkları ve toplamları Çizelge 4.1.'de gösterilmektedir. Paketin kaynak adreslerine göre işaretlenmiş paket sayıları ise Çizelge 4.2.'de gösterilmektedir.

Çizelge 4.1. İşaretlenmiş Paket Sayıları

Kaynak Adres	Yönlendirici Giriş Ara Yüz Adresi	Yönlendirici Çıkış Ara Yüz Adresi	Toplam Paket Sayısı
192.0.4.2	192.0.4.1	192.0.18.2	533
192.0.4.2	192.0.20.2	192.0.1.1	647
192.0.4.2	192.0.18.1	192.0.20.1	646
192.0.15.1	192.0.20.2	192.0.1.1	38
192.0.15.1	192.0.16.1	192.0.20.1	44
192.0.15.1	192.0.15.2	192.0.16.2	35
192.0.14.1	192.0.14.2	192.0.10.2	78
192.0.14.1	192.0.12.1	192.0.11.1	58
192.0.14.1	192.0.11.2	192.0.1.1	86
192.0.14.1	192.0.10.1	192.0.12.2	69
192.0.13.1	192.0.6.2	192.0.1.1	594
192.0.13.1	192.0.5.1	192.0.6.1	553
192.0.13.1	192.0.13.2	192.0.5.2	509

Çizelge 4.2. Kaynak Adreslerine Göre İşaretlenmiş Paket Sayıları

Kaynak Adres	Toplam Paket Sayısı
192.0.4.2	1826
192.0.13.1	1656
192.0.14.1	291
192.0.15.1	117

Tüm paketlerin toplamı 3890'dır ve saldırı noktalarında gelen işaretlenmiş paketlerin normal trafik noktalarından gelen işaretlenmiş paketlere oranı 8,534'tür.

Deney 2: Bu deneyde tezde önerilen Dinamik Değişen Paket İşaretleme Olasılığı yöntemi kullanılarak benzetim yapılmıştır. Yönlendirici üzerindeki tüm paket yollarının paket işaretleme olasılıklarının toplamı 0.05 olarak seçilmiştir. Simülasyon 3600 saniye sürmüştür. Paketlerin hangi kaynaktan çıktığı,

işaretlendikleri yönlendiricilerin hangi giriş ve çıkış noktalarını kullandıkları ve toplamları Çizelge 4.3.'te gösterilmektedir. Paketin kaynak adreslerine göre işaretlenmiş paket sayıları ise Çizelge 4.4.'de gösterilmektedir.

Çizelge 4.3. İşaretlenmiş Paket Sayıları

Kaynak Adres	Yönlendirici Giriş Ara Yüz Adresi	Yönlendirici Çıkış Ara Yüz Adresi	Toplam Paket Sayısı
192.0.4.2	192.0.4.1	192.0.18.2	608
192.0.4.2	192.0.20.2	192.0.1.1	226
192.0.4.2	192.0.18.1	192.0.20.1	535
192.0.15.1	192.0.20.2	192.0.1.1	13
192.0.15.1	192.0.16.1	192.0.20.1	12
192.0.15.1	192.0.15.2	192.0.16.2	29
192.0.14.1	192.0.14.2	192.0.10.2	92
192.0.14.1	192.0.12.1	192.0.11.1	87
192.0.14.1	192.0.11.2	192.0.1.1	18
192.0.14.1	192.0.10.1	192.0.12.2	34
192.0.13.1	192.0.6.2	192.0.1.1	302
192.0.13.1	192.0.5.1	192.0.6.1	584
192.0.13.1	192.0.13.2	192.0.5.2	550

Çizelge 4.4. Kaynak Adreslerine Göre İşaretlenmiş Paket Sayıları

Kaynak Adres	Toplam Paket Sayısı
192.0.4.2	1369
192.0.13.1	1436
192.0.14.1	231
192.0.15.1	54

Tüm paketlerin toplamı 3090'dır ve saldırı noktalarından üretilen işaretlenmiş paketlerin normal trafik noktalarından üretilen işaretlenmiş paketlere oranı 9,842'dir.

Daha önceki kısımda da anlatıldığı gibi paketlere zıplama sayısı eklenmektedir. Bu deneyden elde edilen paket işaretlerindeki IP adresleri ve zıplama sayıları Çizelge 4.5.'te gösterilmiştir.

Çizelge 4.5. Zıplama Sayıları ve IP Adresleri

Zıplama Sayısı	IP Adresleri
1920101	192.0.10.1
1920102	192.0.11.2 -192.0.12.1
1920112	192.0.11.2
1920121	192.0.12.1
1920132	192.0.13.2
1920133	192.0.6.2 - 192.0.5.1
1920134	192.0.6.2
1920142	192.0.14.2
1920143	192.0.12.1
1920152	192.0.15.2
1920153	192.0.20.2
1920161	192.0.16.1
1920181	192.0.18.1
1920202	192.0.20.2
192041	192.0.4.1
192042	192.0.20.2 - 192.0.18.1
192043	192.0.20.2
192051	192.0.5.1
192052	192.0.6.2
192062	192.0.6.2

Zıplama sayılarına bakılarak yapılan geri izleme işleminin sonucunda bulunan yollar Şekil 4.16. 'da gösterilmiştir.

```
YOL
192.0.20.2 --> 192.0.18.1-->
YOL
192.0.16.1 -->
YOL
192.0.20.2 --> 192.0.15.2 -->
YOL
192.0.12.1 --> 192.0.14.2 -->
YOL
192.0.6.2 --> 192.0.5.1 --> 192.0.13.2 -->
YOL
192.0.12.1 -->
YOL
192.0.11.2 -->
YOL
192.0.11.2 --> 192.0.12.1 --> 192.0.10.1 -->
YOL
192.0.6.2 -->
YOL
192.0.6.2 --> 192.0.5.1 -->
YOL
192.0.20.2 --> 192.0.18.1 --> 192.0.4.1 -->
```

Şekil 4.19. Geri İzleme İşleminin Sonucu

Gerçek saldırı yolları olan “192.0.20.2 --> 192.0.18.1 --> 192.0.4.1” ve “192.0.6.2 --> 192.0.5.1 --> 192.0.13.2 ” Şekil 4.4.’te gösterilen geri izleme işlemi kullanılarak bulunmuştur.

5. SONUÇ

Bu çalışmada, günümüzün en önemli veri ağ güvenlik sorunu olan (D)DoS saldırında saldırıların asıl kaynaklarını bulmak için literatürde önerilen IP geri izleme yöntemleri üzerinde çalışılmıştır. Literatürde önerilen IP geri izleme yöntemleri arasında kullanılabilirliği ve var olan veri ağ altyapısına uygunluğu en çok olan yöntemin Paket İşaretleme yöntemi olduğu görülmüştür. Diğer yöntemlerin uygulanması için var olan veri ağı alt yapısında değişiklikler yapılmalı veya bant genişliğinden büyük ödünler verilmelidir. Fakat paket işaretleme yöntemi için sadece yönlendiricilerde yapılacak bir yazılım güncellemesi yeterli olacaktır. Paket işaretleme yönteminde işlem yükünün çoğunu, saldırıların hedefi olan bilgisayar yaptığı için yönlendiriciler temel görevleri olan paket yönlendirme işlemlerinde yavaşlama olmayacaktır. Bu tezde, Olasılıksal Paket İşaretleme (Probabilistic Packet Marking, PPM) yöntemini geliştirmek için yeni çözüm yolları üzerinde çalışılmıştır. Literatürde önerilen PPM yönteminde yönlendiriciye gelen her hangi bir paket sabit bir olasılıkla işaretlenmekteyken bu tezde önerilen yöntemle gelen paketler yönlendiriciye girdikleri ve çıktıkları noktalar gözlenerek bu noktalar arasındaki trafik yoğunluğuyla doğru orantılı değişen olasılıkla işaretlenmiştir. Saldırı sırasında paket sayıları artacağından, saldırı paketlerinin geçtiği yönlendiricilerde bu paketlerin işaretleme olasılığı, normal trafik yollarına göre daha fazla olması amaçlanmıştır.

Bu tezde önerilen paket işaretleme yöntemini ve literatürde önerilen PPM yöntemini karşılaştırmak amacıyla OPNET simülasyon yazılımıyla veri ağı topolojisi oluşturulmuştur. Oluşturulan veri ağında her iki yöntemde çalıştırılmıştır. Yapılan deneyler sonucunda, bu tezde önerilen paket işaretleme yöntemi kullanıldığında saldırı noktalarını belirlemek için gereken işaretlenmiş paket sayısın daha az olduğu görülmüştür. Toplam işaretlenmiş paket sayısının daha az olması demek yönlendiricilere daha az iş yükü anlamına gelmektedir. Ayrıca saldırı noktalarından gelen işaretlenmiş paket sayılarının normal noktalardan gelen işaretlenmiş paket sayılarına oranının daha büyük olduğu görülmüştür. Aynı yönlendirici tarafından işaretlenen paketlerin birbirlerine

oranlarına bakılarak saldırının yönlendiricinin hangi ara yüz noktasından girdiği tespit edilebilmiştir.

Literatürde önerilen PPM yönteminde paketlere sadece yönlendiricin giriş ara yüz adresi eklenmektedir. DDoS saldırılarından hedefi olan bilgisayar işaretlenmiş paketleri açtığında sadece IP adreslerini bulmaktadır. Hedef bilgisayarın saldırı yollarını belirlemesi için yönlendiricilerin ara yüz IP adreslerini ve yönlendiricilerin paket akışındaki sırasını bilmesi gereklidir. DDoS saldırıları birden fazla veri ağı yolu ve nokta kullanılarak yapıldığından bu farklı veri ağı yollarının bulunması için paket işaretlerine bu yolları ayırt edebilecek bir bilgi eklenmelidir. Bu amaçla paket işaretlerine zıplama sayısı eklenmiştir. Zıplama sayıları, işaretlenmiş paketler tekrar işaretlenince arttırıldığından aynı paket akışının olduğu yönlendiricilerin işaretlediği paket işaretleri birbirlerine yakın sayılardan oluşacaktır. Yapılan deneyler sonucunda elde edilen zıplama sayılarına bakılarak paket akış yolları bulunmuştur. Literatürde önerilen PPM yönteminde elde edilen IP adresleriyle ne yapılacağı ile ilgili eksiklik zıplama sayısı eklenerek giderilmiştir.

Paket işaretleri, IP paketlerin opsiyonlar ve dolgu (options and padding) kısmına eklenmiştir. Eklenen paket işareti, paket boyutunu sekiz bayt büyütmesine rağmen bu tezde önerilen paket işaretleme olasılığı, literatürde önerilen PPM yöntemine göre toplamda daha az paket işaretlediğinden bant genişliğindeki bu azalma göz ardı edilebilir.

İleride bu çalışmada önerilen paket işaretleme yönteminin kullandığı paket işaretinin getirdiği yükü azaltmak için farklı yöntemler geliştirilebilir. IP Datagram'da çok az kullanılan kısımlarda paket işaretleri saklanabilir. Böylece bant genişliğinde hiçbir azalma olmaksızın bu tezde önerilen paket işaretleme yöntemi kullanılabilir. Paketlerdeki işaretlerin bozulmasını veya değiştirilmesini engellemek için güvenlik yöntemleri geliştirilebilir. Ayrıca zıplama sayıları üzerinde daha derinlemesine durulup yeni yöntemler bulunabilir.

KAYNAKLAR

[1] Anonim, Denial of Service Attacks, 2008. http://www.cert.org/tech_tips/denial_of_service.html

[2] Lehrer, D., *Trafic Jam*, 2000. http://www.pbs.org/newshour/bb/cyberspace/jan-june00/yahoo_2-8.html

[3] Ferguson, P., "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing," IETF RFC 2827, 2000.

[4] Anonim, *Network intrusion detection system*, 2008. http://en.wikipedia.org/wiki/Network_intrusion_detection_system

[5] Savage, S., D. Wetherall, A. Karlin, ve Anderson, T., "Practical network support for ip traceback," ACM SIGCOMM, 2000.

[6] Bellovin, S.M., "ICMP Traceback Messages," IEFT draft, 2000.

[7] Snoeren et al., A. C., "Single-Packet IP Traceback", IEEE/ACM Trans.Net., **10**(6), 721–34, 2002.

[8] Burch, H. ve Cheswick, B., "Tracing Anonymous Packets to Their Approximate Source," Proc. USENIX LISA, 319–27, 2000.

[9] Stone, R., "CenterTrack: An IP Overlay Network for Tracking DoS Floods," USENIX Security Symposium, Denver, 2000.

[10] Postel, J., "Character Generation Protocol," IETF RFC 864, 1983.

[11] Belenky, A. ve Ansari, N., "IP traceback with Deterministic Packet Marking," IEEE Communications Letters, **7**(4), 162-164, 2003.

[12] Postel, J., "Internet Protocol," IETF RFC 791, 1981.

[13] Song, D.X. ve Perrig A., "Advanced and Authenticated Marking Schemes for IP Traceback," Proc. INFOCOM, **2**, 878–86, 2001.

[14] Anonim, *OPNET Modeler*, 2008. http://www.opnet.com/solutions/network_rd/modeler.html