T.C.
BEYKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
BİLGİSAYAR MÜHENDİSLİĞİ BİLİM DALI

YENİ NESİL İNTERNET PROTOKOLÜ IPv6'DA GÜVENLİK RİSKLERİ VE OLASI ÇÖZÜM ÖNERİLERİ

YÜKSEK LİSANS TEZİ

ALİ EFE

İstanbul, 2006

T.C.
BEYKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
BİLGİSAYAR MÜHENDİSLİĞİ BİLİM DALI

YENİ NESİL İNTERNET PROTOKOLÜ IPv6'DA GÜVENLİK RİSKLERİ VE OLASI ÇÖZÜM ÖNERİLERİ

YÜKSEK LİSANS TEZİ

ALİ EFE

TEZ DANIŞMANI: Dr. RİFAT ÇÖLKESEN

İstanbul, 2006

T.C.
BEYKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜ
YÜKSEK LİSANS TEZ SINAV TUTANAĞI

06./03./2006

Enstitümüz ***Bilgisayar Mühendisliği Anabilim Dalı Bilgisayar Mühendisliği Bilim Dalı*** yüksek lisans öğrencilerinden BM2351-001 numaralı ***Ali Efe'nin*** *"Beykent Üniversitesi Lisansüstü Eğitim - Öğretim ve Sınav Yönetmeliği"* nin ilgili maddesine göre hazırlayarak, Enstitümüze teslim ettiği ***"YENİ NESİL İNTERNET PROTOKOLÜ IPv6'DA GÜVENLİK RİSKLERİ VE OLASI ÇÖZÜM ÖNERİLERİ"*** adlı tezi, Yönetim Kurulumuzun 06.03.2006 tarih ve 2006/03 sayılı toplantısında seçilen ve Enstitü binasında toplanan biz jüri üyeleri huzurunda, Lisansüstü Eğitim-Öğretim ve Sınav Yönetmeliğinin 27-c *maddesi gereğince* (.60..) dakika süre ile aday tarafından savunulmuş ve sonuçta adayın Tezi hakkında ***oybirliği*** ile ***Kabul*** kararı verilmiştir.

İşbu tutanak, 5 nüsha olarak hazırlanmış ve Enstitü Müdürlüğü'ne sunulmak üzere tarafımızdan düzenlenmiştir.

DANIŞMAN
YRD.DOÇ.DR.RİFAT ÇÖLKESEN

ÜYE
PROF.DR.ESAT HAMZAOĞLU

ÜYE
PROF.DR.BÜLENT ÖRENCİK

ÖZGEÇMİŞ

Ali EFE, 1980 Yılında Herisau/İsviçre'de doğdu. Lise eğitimini Özel Selim Pars Fen Lisesinde tamamladıktan sonra Pamukkale Üniversitesi Makine Mühendisliği bölümünde lisans eğitimini tamamladı. Bilgi teknolojileri ve bilgisayar ağları konusunda duyduğu yoğun merak ve bu alanda çalışma isteği sonucunda bu konuda eğitim alma kararı verdi ve 2003 yılında Beykent Üniversitesi'nde Bilgisayar Mühendisliği Yüksek Lisans eğitimine başladı. "Her zaman öğrenilecek çok şey vardır" mantığını benimseyen EFE, bilgisayar ağları, ağ/bilgi güvenliği ve programlama konularına ilgi duymakta ve bu konuda kendini geliştirme çalışmalarına devam etmektedir.

ÖNSÖZ

İnternet şüphesiz ki bilgiye en kolay ve en hızlı ulaşım kaynağı olmuştur. Bunun yanında yakın zamanda bireylerin birçok ihtiyaçlarını İnternet ortamından karşılaması da beklenmektedir. Örnek olarak gelecekteki evlerde İnternet üzerinden otomasyon sistemleri çalışacak ve bireyler yaşamlarında kullandıkları irili ufaklı bir çok cihazı kendi kişisel ve taşınabilir bilgisayarlarından yönetebilecekler, diğer bireylerle her an heryerden görüntülü olarak görüşebilecekler ve İnternet üzerinden alışveriş ihtiyaçlarını karşılayacaklardır. Bu açıdan düşünüldüğünde İnternet'in temelinde yatan protokoller ve bunlardan en önemlisi olan İnternet Protokolünün önemi daha da anlaşılmaktadır. Bu çalışmada yeni nesil internet protokolü olan IPv6 güvenlik riskleri açısından ele alınarak incelenmiş ve bazı öngörüler sunulmuştur. Bu çalışmanın her aşamasında bilgi ve deneyimleriyle bana yol gösteren sayın hocam Yrd. Doç. Dr. Rifat ÇÖLKESEN'e, tezin tamamlanma aşamasında önerileriyle katkıda bulunan sayın Prof. Dr. Esat HAMZAOĞLU'na, yoğun temposuna rağmen zaman ayıran ve değerli fikirleriyle çalışmamızın geleceğine yönelik katkı sağlayan sayın Prof. Dr. Bülent ÖRENCİK'e ve son olarak da desteklerini esirgemeyen aileme teşekkürü borç bilirim.

İstanbul, 2006 Ali EFE

İÇİNDEKİLER

Sayfa No.

ŞEKİL LİSTESİ

KISALTMALAR

OSI	:	Open Systems Interconnection
QoS	:	Quality of Service – Servis Kalitesi
IETF	:	Internet Engineering Task Force – İnternet Mühendisleri Çalışma Kolu
NAT	:	Network Address Translation – Ağ Adres Dönüşümü
NAT-PT	:	NAT with Protocol Translator – Protokol Dönüştürücülü Ağ Adres Dönüşümü
DoS	:	Denial of Service – Servis Engelleme
DDoS	:	Distributed Denial of Service – Dağıtık Servis Engelleme
ICMP	:	Internet Control Message Protocol – İnternet Kontrol Mesajı Protokolü
ISP	:	Internet Service Provider – İnternet Servis Sağlayıcısı
IP	:	Internet Protocol – İnternet Protokolü
TTL	:	Time to Live – Yaşam Süresi
RFC	:	Request for Comments
IANA	:	Internet Assigned Numbers Authority – İnternette Tanımlanmış Numaralar Otoritesi
TLV	:	Type-Length-Value – Tür-Uzunluk-Değer
MTU	:	Maximum Transmission Unit – Maksimum İletim Birimi
ICV	:	Integrity Check Value – Bütünlük Kontrol Değeri

IPSec	:	IP Security Protocol – IP Güvenlik Protokolü
MAC	:	Media Access Control – Ortam Erişim Kontrolü
ARP	:	Address Resolution Protocol – Adres Çözümleme Protokolü
DHCP	:	Dynamic Host Configuration Protocol
DNS	:	Domain Name System
NTP	:	Network Time Protocol
OSPF	:	Open Shortest Path First – İlk En Kısa Açık Yol
AH	:	Authentication Header – Doğrulama Başlığı
ESP	:	Encapsulating Security Payload – Emanet Verinin Paketlenmesi Başlığı
IKE	:	Internet Key Exchange – İnternet Anahtar Değiştokuş protokolü
ISAKMP	:	Internet Security Association and Key Management Protocol – İnternet Güvenlik Birliği ve Anahtar Yönetimi Protokolü
IDS	:	Intrusion Detection System – Saldırı Tespit Sistemi

ÖZET

OSI referans modeline göre 3. katmanda çalışan ve paketlerin ağ üzerinde belirlenmiş hedefler üzerinden aktarımında kullanılan protokol İnternet Protokolü(IP)' dür. Günümüzde kullanılan İnternet Protokolü ise IPv4'dür. Bu protokol 1981 yılında RFC 791 ile tanımlandığı gibi standartlaşmıştır. Fakat İnternet'in beklenenden çok daha hızlı gelişmesi ve yaygınlaşması beraberinde çeşitli problemleri ve beklentileri de getirmiştir. Bu problemlere yönelik çözüm çalışmalarının sonucunda yeni bir İnternet Protokolü geliştirilmiş ve 1995 yılında IPv6 adı verilerek standartlaştırılmıştır. IPv4'ün mimarisi gereği eksik kaldığı noktalarda IPv6 çare getirmesi hedeflenen bir çalışma olarak sunulmuştur. Günümüzde de bu protokol yavaş yavaş uygulamaya geçirilmekte ve bir yandan da geliştirme çalışmaları devam etmektedir.

Hazırlanan bu çalışmada IPv6 protokolünün başlık yapısı ele alınmış, bu yeni başlık yapısının ve getirmiş olduğu fonksiyonların uygulamalar ve güvenlik açısından etkileri tartışılmıştır. Çalışmada sırasıyla; IPv6 teknolojisi üzerinde yapılan bazı çalışmalar hakkında bilgi verilmiş, IPv6 temel başlığı ve ek-başlıklarının yapısı irdelenmiş, bu başlık yapılarında sağlanan fonksiyonellik sayesinde uygulamalara etkisinin nasıl olacağı konusunda bazı öngörülerde bulunulmuştur. Ardından günümüzde İnternet ortamında yaşanan saldırılar ve güvenlik sorunları hakkında bilgi verilmiş, IPv6 teknolojisine geçiş sonrasında bu tehditlerde değişiklik olup olmayacağına yönelik beklentiler aktarılmıştır. Çalışmanın son bölümünde ise yeni protokol ve başlık yapılarına bağlı olarak ve de önceki bölümlerde sunulan bilgiler ışığında, IPv6'da ne gibi yeni saldırıların olabileceğine yönelik yaptığımız öngörüler yer almaktadır. Bu öngörülerimizden biri olan ve Ping-Pong saldırısı olarak adlandırdığımız saldırı ayrıca ele alınmış ve bu konuda bir çözüm önerisi de çalışmada sunulmuştur.

ABSTRACT

According to OSI reference model, transferring data between the nodes works on the 3rd layer and is called Internet Protocol (IP). Currently the Internet Protocol is used IPv4. This protocol has been standardized in 1981 as outlined in RFC-791. Yet fast improvement of usage of Internet more than expected has also introduced some inherent and unexpected problems. In order to solve the above given problems, studies have been carried out and as a result a new Internet Protocol has been emerged in 1995, the name IPv6 was given to it and standardized. As is known, architecture of IPv4 when compared to IPv6 is insufficient and IPv6 is seen as brand new and offers broad novelties when compared to its predecessor. Currently implementation of IPv6 occurs slowly and steadily and yet improvements in IPv6 are not complete and still in progress.

In this study, header structure of IPv6 protocol has been taken into consideration and the novelties presented by the new header structure such as applications and security related problems have been discussed. First of all, information related to IPv6 were given, structure of IPv6 standard header and extension headers were investigated. The functions related to header structure and their effects were investigated and some predictions were also presented. Then, information about attacks related to Internet and some security problems are presented. Having gone through IPv6 technology, if expectations related to threats mentioned above are going to still remain or changed is considered. In the last part of the studies, in relation to new protocol and header structure and the light of knowledge presented in the previous sections, what kind of new attacks towards IPv6 may take place is predicted? According to one of the predictions whose name is given by us to be “ping-pong” attack has been treated separately and a solution to this problem is proposed.

1. Giriş

OSI referans modeline göre 3. katmanda çalışan ve paketlerin ağ üzeride çeşitli ara düğümlerden geçerek belirlenmiş hedefe aktarımında kullanılan protokol kısaca IP (İnternet Protokolü)'dir. Günümüzde kullanılan uyarlaması ise IPv4'dür. Bu protokol 1981 yılında RFC 791 ile tanımlandığı gibi standartlaşmıştır. Fakat İnternet'in beklenenden çok daha hızlı gelişmesi ve yaygınlaşması beraberinde çeşitli problemleri ve ek beklentileri de getirmiştir. IPv4'ün mimarisi gereği eksik kaldığı noktalarda IPv6 çare getirmesi hedeflenen bir çalışma olarak sunulmuştur. Bu problemlere yönelik çözüm çalışmalarının sonucunda yeni bir İnternet Protokolü geliştirilmiş ve 1995 yılında IPv6 adı verilerek standartlaştırılmıştır. Günümüzde de bu protokol yavaş yavaş uygulamaya geçirilmekte ve bir yandan da geliştirme çalışmaları devam etmektedir.

IPv6'da paketin başlık yapısı IPv4'e göre değiştirilmiştir. IPv4'de paket başlığında kullanılan bazı alanlar IPv6'da bulunmamaktadır; ayrıca ek başlık adı altında eklemeler yapılmıştır. IPv6'da paketin temel-başlık yapısında sadeleşme göze çarpmakla birlikte, IPv6'nın esas getirileri temel başlık paketinin arkasına zincir gibi bağlanmak suretiyle eklenebilen ek-başlık yapısı incelendiğinde göz önüne çıkmaktadır.

IPv6'da yenilikler:

- Yeni başlık yapısı (Ek-başlıklar olması)
- Geniş adres aralığı (128-bitlik adresler)
- Verimli, hiyerarşik adresleme ve yönlendirme altyapısı
- Bağlantısız veya bağlantıya yönelik adres atama işlemi
- Başlık yapısı içerisinde desteklenen güvenlik

- Daha iyi QoS desteği
- Komşu düğüm iletişimi için yeni protokol (IPv4'deki ARP yerine)
- Ölçeklenebilirlik

1.1 IPv6 Üzerine Yapılan Çalışmalar

IPv4 üzerine geliştirilen kablosuz ağlar tüm dünyada hızla kullanılmaya başlanmıştır. Fakat IPv4'ün başlangıçta adres aralığı konusundaki sıkıntılarına çözüm olarak sunulan IPv6'ın kullanıma geçmesiyle birlikte, IPv6 kullanan sistemlerin ilk etapta, mevcut IPv4 yapısı üzerinden birbirleriyle veya IPv4 ve IPv6 kullanan sistemlerin birbirleriyle haberleşebilmesi için geçiş çalışmaları sürmektedir. Araştırmacılar bu çalışmalarında IPv4'den IPv6'ya geçiş mekanizmalarını incelemiş, ardından da saydam (transparent) IPv6 (TIP6) olarak adlandırılan ve geliştirilmiş bazı mekanizmaların getirilerinin birlikte bir yapı içerisinde kullanımına dayanan bir mekanizma sunmuşlardır. Bu mekanizmanın amacı IPv4 sistemler üzerinde değişiklik yapılmadan IPv6 adreslemesi kullanılabilmesi, sistemlerin kademeli olarak yeni altyapıya geçirilmesidir. Bu amaçla IETF'un geliştirdiği "6to4" ve NAT-PT mekanizmaları birlikte kullanılmış. Son olarak araştırmacılar bu çalışmada sundukları Saydam IPv6 mekanizmasının Mobil IP hücresel teknolojilerinde (GPRS ve IDEN) herhangi bir değişiklik gerektirmeden kullanılabileceği öngörüsünde bulunmuşlar.[1]

WADDINGTON, D. G. ve CHANG, F. isimli araştırmacılar da yaptıkları çalışmada IPv4'den IPv6'ya geçiş sürecini ve bu iki protokolün geçiş süresince birlikte kullanılması üzerine çalışma yapmışlardır [2]. SAMAD M., YUSUF F., HASHIM H., ve Md ZAN Md M. isimli araştırmacılar da iki protokolün birlikte kullanıldığı ve çift yığınlı sistemli çözümlerle yapılacak geçiş yöntemlerini incelemiş ve çalışmalarında yaptıkları uygulamaları sunmuşlardır [3].

IPv6'nın yayılmasıyla birlikte doğal olarak çeşitli sunucular da bu teknolojiye uyum sağlayacaktır. Bunun için çalışmalar yürütülmektedir. Bunlardan en önemli konumda olan sunuculardan biri de hiç şüphesiz Web-sunucularıdır. Bu konuda dünya çapında yaygın olarak kullanılan Web sunucusu yazılımı Apache, 2.0 sürümünden itibaren IPv6 protokolünü bünyesinde desteklemektedir [18]. NAKAYAMA, T., NAKAMURA, Y., SUNAHARA, H. adlı araştırmacılar 2003 yılında gerçekleştirilmiş olan Uygulamalar ve İnternet Çalışmaları Sempozyumu'nda (SAINT-w'03: Symposium on Applications and the Internet Workshop 2003) sunmuş oldukları çalışmada Apache 1.3.27 sürümü ve resmi olmayan IPv6 yamasının kullanıldığı bir sunucu sistem üzerinde IPv6 performansını sınamışlardır. Bu testte o an için var olan herhangi bir kıyaslama testi (benchmark) yazılımının IPv6 desteği sunmaması sonucunda kendi kıyaslama sistemlerini geliştirmişler ve bu sistemin bir ayağı olan ANMA olarak adlandırdıkları bir istemci yazılımı geliştirmek suretiyle bir test ortamı yaratmışlardır. Araştırmacılar yaptıkları çalışmaların sonucunda IPv6'da bağlantı sağlanması işlem süresinin IPv4'dekine oranla ortalama 10 kat daha yavaş olduğunu (0.01ms), RTT olarak adlandırılan, bağlantı kurulup verinin iletildiği ve bağlantının sonlandırılmasını kapsayan sürede IPv6'nın yaklaşık 7ms daha yavaş kaldığını bulmuşlar. Bu çalışmada sunucuda 4 KB büyüklüğünde dosya kullanılmış. Ayrıca her iki protokol için iletişim süresince aktarılan paketlerin yaklaşık %10'unun RST paketi olduğunu görülmüş ve performans değerlendirmelerinde bu paketler göz ardı edilmiş. [4]

COCQUET, P. İsimli araştırmacı 9 Eylül 2004'de (IEEE Yayınları Sayı:92 No:9'da) yayınlanan "DSL'de IPv6: Daima Hazır Servisler Ortaya Çıkarmanın En İyi Yolu" adlı makalesinde geniş band iletişiminin Telekom kurumları, servis sağlayıcıları ve ekonomide rolü açısından önemine vurgulanmış ve IPv6'nın bu iletişim ortamında kullanılabilirliği üzerinde çalışmaların yapıldığı vurgulanmış. Yazar, yeni nesil protokolün yalın halde kullanımının beklenmesine gerek kalmadan, geçiş sürecinde bile, operatörler ve servis sağlayıcılar tarafından daha zengin servislerinin sağlanabileceğini ve bunun getirisi olarak yeni iş modellerinin ortaya çıkacağı öngörüsünde bulunmuştur. Çalışmasında DSL servisleri üzerinde IPv6'nın kullanılmasına yönelik mimarileri incelemiş, geliştirilen bu mimariler sayesinde geçiş sürecinin yumuşak bir şekilde gerçekleştirilebileceğini ortaya

koymuştur. Servis sağlayıcıların iletişim omurgalarında NAT-PT gibi teknolojileri kullanmasıyla sadece IPv6 kullanan terminallerin İnternet'teki sadece IPv4 kullanan kaynaklara erişebileceği vurgulanmıştır. [5]

IPv6'nın kullanılmasına yönelik geliştirme çalışmalarında hiç şüphesiz ki uç sistemlerde kullanılan işletim sistemlerin uyumluluğu ve performansı da çok önemli bir kriter teşkil etmektedir. Günümüzde yaygın olarak kullanılan gelişmiş tüm işletim sistemleri IPv6'ya bünyesinde destek vermektedir. Peki, bu işletim sistemlerinin bu konudaki başarıları ne durumdadır? ZEADALLY,S., WASSEEM,R ve RAICU, I. isimli araştırmacılar Haziran 2004'de yayınlanan çalışmalarında 3 popüler işletim sistemi olan Windows 2000, Linux ve Solaris 8 işletim sistemlerini, kullandıkları IPv6 protokol yığınlarındaki performansları açısından değerlendirmiş ve karşılaştırmışlardır. Bu çalışmanın sonucuna göre TCP/IPv4 ve TCP/IPv6 soket oluşturma sürelerine göre Linux işletim sistemi Windows 2000 işletim sistemine kıyasla 16 ve 19 kat, Solaris 8 işletim sistemine kıyasla 4 kat daha fazla performans sağlamaktadır. Yine aynı çalışmada yapılan Web simulasyonu sonucunda Linux ve Solaris 8 işletim sistemleri IPv6'da Windows 2000 işletim sistemine oranla 4 katlık bir performans artışı gösterdiği saptanmış. [6]

İnternet ortamında güvenlik hiç şüphesiz en önemli noktalardan biridir. IPv6'nın gelişiyle birlikte günümüzde İnternet'te yaşanan güvenlik sorunlarının gelecekte nasıl bir eğilim göstereceği de merak konusudur. Bu konuda yapılan çalışmalardan biri de LEE,C.J.Henry, MA,M., THING, L.L.V, XU,Y. isimli araştırmacılara aittir. Araştırmacılar günümüzde en kolay uygulanabilen ve dolayısıyla yaygın saldırılardan biri olan Hizmet Engelleme (DoS) ve Dağıtık Hizmet Engelleme Saldırılarını (DDoS) engellemeye yönelik kilit noktalarından birinin saldırı kaynağının tespit edilebilmesi olduğuna dikkat çekmişlerdir. DoS saldırıları Symantec şirketinin düzenli olarak yayınladığı Güvenlik Tehditleri Mart 2005 tarihli raporunda İnternet'te karşılaşılan en büyük ikinci saldırı olarak nitelendirilmiştir [19]. Bu çalışmada geriye yönelik iz sürme (traceback) yöntemlerinin IPv6 ve Mobil IPv6'daki uygulanabilirliği ele alınmıştır. Yazarlar İnternet'in doğası gereği geriye yönelik iz sürme yöntemlerinin kolay ve kesin sonuç veremediğine dikkat çekmişler

ve IPv6 teknolojisi için bu yöntemde yaşanacak en büyük sıkıntıların uygulanacak adres dönüşüm işlemleri, yani tünelleme ve adres üzerinde değişiklik işlemlerinden kaynaklanacağı fikrini ileri sürmüşlerdir. Ayrıca bu çalışmalarında önerdikleri yeni bir ICMPv6 paketi ile koordinasyonun sağlandığı yeni bir geriye yönelik iz sürme tekniği önermişlerdir. Mobil IPv6'ya yönelik ise yazarlar Mobil düğümlerin saldırılar için istismara açık olduklarını ve bunun da geriye yönelik iz sürme çalışmalarını başarısız kılabileceğini belirtmişler ve bu soruna çözüm olarak da Mobil IPv6 düğümler ile bağlı oldukları "Home Agent" cihazı arasında doğrulama yapılarak oluşturulmuş ve tünellenmiş bir bağlantı kullanılmasını önermişlerdir. [7]

IPv6'nın uygulamaya geçişiyle birlikte hiç şüphesiz ki bir noktadan çok noktaya yönelik iletişim (*multicast*) daha önem kazanacaktır. METZ, C. ve TATIPAMULA, M. isimli araştırmacılarda bu noktaya dikkat çekmişlerdir. "*Multicast* türü trafiğin aynı anda paralel olarak aynı verinin iletilmesi gereken heryerde -video konferans, şirket iletişimleri, uzaktan eğitim, dağıtık sistemlerde çalışan yazılımlar, haberler vb.- kullanılacaktır" diyen yazarlar çalışmalarında IPv6'da *multicast* iletişim şeklini ele almışlar ve alanlar arasında kullanımının nasıl olacağını incelemişlerdir. Yazarlar *multicast* trafiğin uygulanmasına yönelik Avrupa çapında M6Bone araştırma ağının ve 6NET projesi çerçevesinde oluşturulan iletişim ağının bu türdeki trafiğe yönelik yapılacak çalışmalar için destek sağladığını belirtmişlerdir. Japon Sky Perfect Communication şirketi 2003 yılında, Sky Stream adını verdikleri IPv6-*Multicast* tabanlı video-yayın servisi projesini harekete geçişmişlerdir. Yine Japonya'da NTT-Communication ve NTT-East adlı servis sağlayıcıları da tanımlanmış doğal IPv6 *multicast* desteği vermeye başladıklarını duyurmuşlardır. [8] Donanım tarafında ise Juniper Networks ve Cisco Systems bazı ürünleriyle birlikte IPv6 desteği sunmaktadırlar.

Yeni nesil protokole geçişle birlikte video aktarımı gibi bazı gerçek zamanlı uygulamaların kullanım alanının daha da yaygın hale gelmesi beklenmektedir. Yapılan literatür araştırması esnasında LEE C. C., CHAN S. W., CHANG P. C. isimli araştırmacıların kablosuz IPv6 ağlarda değişken boyutlu *datagramlar* kullanılması suretiyle

video verilerinin aktarımında, performansa yönelik iyileştirme çalışmaları yaptıklarını gördüm. Bu çalışmalarında yazarlar IPv6'nın geniş adresleme desteği sunmasıyla her düğümün eşi olmayan bir IP adresine sahip olabilmesi ve QoS desteğinin gerçek zamanlı uygulamalar için daha ideal bir ortam oluşturacağına dikkat çekmişlerdir. [9]

IPv6'nın paket yapısı çerçevesinde IPSec desteği vermesiyle birlikte IPSec protokolünün güvenirliliği daha fazla önem kazanmıştır. İncelemelerimde IPSec protokolünün güvenirliğine yönelik risk oluşturabilecek önemli noktaların, bu protokol içerisinde kullanılan IKE anahtar değişimi protokolü çerçevesinde paylaşılmış ortak anahtar (preshared keys) kullanılması durumunda ve yineleme engeli işleminin gerçekleştirilebilmesi için işlem esnasındaki pencere kaydırma suretiyle veri doğrulama esnasında oluşabileceğini gördüm. ZHAO F. ve WU F. S. adlı araştırmacılar da yaptıkları çalışmada, yineleme engeli işleminde kullanılan pencereleme metodu dolayısıyla karşıdan düzgün fakat geç gelen paketlerin değerlendirilmeden yok edilebileceğine dikkat çekmişlerdir. Yaptıkları çalışmada farklı yeniden sıralama modelleri için performans değerlendirmesi gerçekleştirmişlerdir. Her bir model için simulasyon ile performans ve verimlilik karşılaştırması yapmışlar ve daha iyi performans sağlanabilmesi için bazı fikirler öne sürmüşlerdir. Yaptıkları simulasyon testleri sonucunda kendi önerdikleri modelin IPSec kullanıldığı zaman band genişliği kullanımı açısından daha verimli olduğunu görmüşler ve bu çalışmalarını performansa yönelik iyileştirme anlamında umut verici olarak nitelendirmişlerdir. [10]

Diğer çalışmalardan biri de ileride karşılaşacağımız yüksek hızlı İnternet'in donanım kısmına yönelik bir çalışmadır. YAZAKI T., KANETAKE T., AKAHANE S., SAKATA Y., SUGAI K., ve YANO H. adlı araştırmacılar kablolu ortamda yapılan çalışmalar sonucunda 10 Gbps Ethernet ağlarda yönlendirme ve anahtarlama işleminin yapılabildiğini, yeni nesil yönlendirici ve anahtarlarda QoS mekanizmasına ilave olarak akış filtreleme ve akış istatistiğinin toplanması ile oluşturulan mimarinin kullanılmasıyla 320 Gbps seviyesinde hızlara erişilebileceğini belirtmişlerdir. [11]

Bazı ülkelerde IPv6 çalışmaları başlamıştır ve bunlar için araştırma fonları kurulmuştur. Buna örnek olarak Avrupa Birliği oluşturduğu 90 Milyon Euro'luk bir fon ile IPv6 üzerindeki araştırma geliştirme çalışmalarını desteklemektedir. Kurulan geniş çaplı araştırma ağları üzerinde araştırma geliştirme çalışmaları devam ederken, bir yandan da güç hatları üzerinden IPv6 iletişimi, IPv6'da *multicast* iletişime yönelik çalışmalar ve ticari geliştirme projeleri gerçekleştirilmektedir. Avrupa Birliği'nin IPv6 üzerindeki araştırma geliştirme çalışmalarına yönelik gerçek anlamda en önemli adımın GÉANT (Gigabit Pan-Europan Research and Education Network) projesi olduğu belirtilmektedir. Bu ağ 2003'ün başlarında çift protokolü (dualstack) destekleyen 10Gbps altyapıya kavuşmuştur. 2004 yılında ulusal çapta 18 araştırma ve geliştirme ağı GÉANT omurgasına bağlıydı. Günümüzde ise 30 ulusal ve bölgesel araştırma ve eğitim ağı bu omurgaya bağlıdır [20]. GÉANT projesi 4 yıllık bir projedir ve 14–15 Haziran 2005 tarihinden itibaren GÉANT2 adı altında çalışmalara devam edilecektir [21].

Türkiye GÉANT2 konsorsiyumu içerisinde yer almakta ve bu araştırma ağı omurgasına 622Mbps kapasiteli bir hat ile bağlanmaktadır. Bu çıkışı Türkiye'de TÜBİTAK çatısı altında ULAKBİM sağlamaktadır. Bu bağlantı kapasitesinin 2006–2007 yıllarında 2,5Gbps'e çıkarılması hedeflenmektedir.[26]

Bu çalışmaya ek olarak Avrupa çapında 6NET ve Euro6IX projeleri de geliştirilmiştir. Bu projelerde oluşturulan ağ altyapısında doğal IPv6 kullanılmakta ve araştırmacılara araştırma ve geliştirme ortamı sunulması hedeflenmiştir. 6NET projesinin 1 Ocak 2002 ile 31 Aralık 2004 tarihleri arasında yürürlükte olması öngörülmüştür [22]. Bu ağlar GÉANT, Abilene (İnternet 2) ve Asya-Pasifik bölgelerindeki bazı IPv6 araştırma ağlarına bağlıdır. 2004 Yılında yayınlanan "Avrupa'da IPv6 araştırma-geliştirme ve ticari çalışmalar" adlı raporda ülkeler ve bu konudaki çalışmaları şu şekilde bildirilmiştir: [12]

Fransa: France Telecom, Araştırma ve Geliştirme çalışmaları kapsamında, VTHDv6 olarak adlandırılan ve ülke içerisinde farklı siteleri birbirine bağlayan bir ağ 1998 yılından beri geliştirilmektedir. Bu ağ ulusal çapta IPv6 ve çift protokol kullanılan yüksek band

genişliğine sahip bir ağdır. Arsys, Cegetel, Gitoyen ve Nerim adlı İnternet servis sağlayıcıları ticari anlamda hizmet sunmaktadırlar. ".fr" uzantılı sitelerde Eylül 2003 tarihinden itibaren IPv6 desteği sunmaktadırlar.

Almanya : Deutsche Telekom ve T-Systems adlı kuruluşlar birkaç yıl öncesinden itibaren IPv6 üzerinde proje çalışmaları yürütmektedirler. Deutsche Telekom endüstriyel ortaklarıyla birlikte IPv6 çalışmalarının ön safhasını bitirmiştir. Space.Net ticari servislerde IPv6 çözümlerini 2003'ün başlarından itibaren sunmaktadır.

İtalya : Telecom Italia Labs., en eski IPv6 denemelerinden biri olan ngnet.it ağı ile tünelleme servisi kullanan 30.000 deneme kullanıcısına destek vermektedir. Wind ve Edisontel adlı kuruluşlar IPv6 çalışmaları yürütmektedirler fakat henüz bu çalışmalar ticari bir zemin oluşturmamaktadır.

Hollanda : XS4ALL adlı ISP, 2002'den beri IPv6 hizmeti vermektedir. Ayrıca Hollanda Ekonomi Bakanlığı IPv6 çalışmaları için bir fon oluşturmuştur.

Portekiz : Portekiz Ulusal Araştırma ve Eğitim Ağı(PUAEA) tarafından kullanılan genel İnternet dönüşüm ağı GigaPIX6, son birkaç aydır PUAEA' ya bağlı olan Vodafone Portekiz, Telepac ve diğer küçük bölgesel operatörler ile ortak çalışmalar yürütmektedir. Bazı firmalar kendi iç erişim ağlarında denemeler yapmaktadır. Telepac, ISDN üzerinde IPv6 ile ilgili deneme çalışmaları yürütmekte ve 2004 yılında IPv6 destekleyen ticari ADSL hizmeti sunmaya hazırlanmaktadır.

İspanya : İspanya'nın en büyük ISP'si olan arsys, IPv6 hizmetini sunmaya 2003'ün Mayıs ayında Madrid' de düzenlenen küresel IPv6 zirvesiyle birlikte başlamıştır. Konferansın gerçekleştirildiği otel, dünyada müşterilerine ücretsiz IPv6 erişim hizmeti sunan ilk otel olmuştur. Diğer ISP'ler 3-6 ay içerisinde ticari servislerini sunmayı planlamaktadırlar. İspanya'nın en büyük elektronik gazetesi olan El Mundo, bir yıldan fazla bir süreden beri içeriğini IPv6 ortamında da sunmaktadır. Fakat bu hizmeti sadece İspanyolca içerik için

vermektedir. Ulusal Ar-Ge fonu 2003'den beri bu konudaki çalışmalara ödenek ayırmıştır. 2004 yılı için daha geniş ödenek ayrılacağı bildirilmiştir.

İsveç : TeliaSonera 2002'den beri ticari hizmet sunmaktadır.

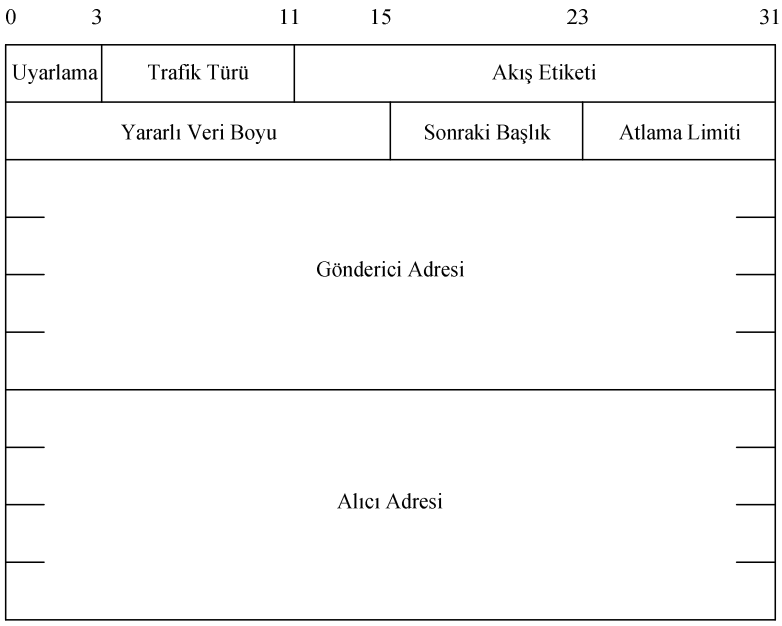
İsviçre : Swisscom Mobile, GPRS/UMTS ile ilk testlerini kablosuz ağ üzerinde yapmaktadır. Ticari anlamda hizmet sunumlarını ise WLAN için 2004, UMTS için 2005 yılında yapmaları beklenmektedir. Haziran 2003'den beri Euro6IX'e bağlı olan Swisscom Enterprise Solutions(iş ortaklarına çözümler sunan ISP) doğal IPv6 üzerinde test çalışmaları yapmaktadır. Bluewin adlı ISP ise Mayıs 2002'den beri denemelerini gerçekleştirmektedir ve 2004–2005 civarlarında ticari hizmetler sunmayı planlamaktadır.

İngiltere : UK6X isimle İnternet geçiş ağı 2002'den beri hizmet sunmaktadır ve telekomünikasyon şirketleri, ISP'ler ve firmalar için bu çalışmalarında kılavuzluk etmektedir. Birleşik Krallığın alan adı tescil merkezi olan (NIC) Nominet, ".uk" uzantılı alanlar için IPv6 desteği vermeyi planlamaktadır.

2. IPv4 ve IPv6 Başlık Yapıları

IPv6'da başlık yapısı önceki uyarlamasına oranla oldukça değişmiştir. Ayrıca yeni başlığın uzunluğu ek-başlıklara ek olarak temel başlık uzunluğu 40 Byte'a çıkmıştır. İki protokolün başlık yapısı kısaca incelenecek olunursa:

Şekil 1. IPv4 Başlık Yapısı



Şekil 2. IPv6 Temel Başlık Yapısı

2.1. IPv6 Temel Başlık Yapısı

Şekil 2'de de görüldüğü gibi yeni nesil İnternet Protokolü IPv6'nın temel başlık yapısında IPv4'ün başlık yapısındaki bazı alanlar çıkarılmış ve daha sade bir yapı elde edilmiştir. Bu başlık yapısında gönderici ve alıcı adreslerinin 128 bit oluşu en çok dikkat çeken farktır. İki başlık yapısında da alıcı ve gönderici adreslerinin tutulduğu alanlar göz ardı edilirse, geri kalan bilgilerin taşındığı alanların büyüklüğü IPv4'de 12 Byte, IPv6'da ise 8 Byte olmaktadır. Bu açıdan bakıldığında IPv6 temel başlık yapısı IPv4'ün başlığına oranla daha küçük gibi görünse de, adreslemenin 128 bit oluşu dolayısıyla, IPv4'de 20 Byte olan toplam IP başlığı uzunluğuna karşı IPv6'da temel başlık toplam 40 Byte olmaktadır. IPv6 temel başlığının yapısı incelenecek olursa tanımlanmış alanlar sırasıyla şunlardır:

Uyarlama: 4 bit uzunluğundadır. Kullanılan İnternet Protokolünün sürümü bu alanda bildirilir.

Trafik Türü: 8 bit uzunluğundadır. IPv6 paketi için belirlenecek trafik türü veya öncelik bilgisi bu alanda taşınır. IPv4'deki *servis türü* alanına benzer bir fonksiyona sahiptir. İlgili RFC'lerce bu alanda kullanılmak üzere herhangi bir değer tanımlanmamıştır.

Akış Etiketi: 20 bit uzunluğundadır. Paketlerin kaynak ile hedef arasındaki aktarımı esnasında belirlenmiş özel bir sıralamada aktarılması, aradaki IPv6 yönlendiricileri tarafından belirtilen bu özel sıralamada değerlendirilmesi için kullanılır.

Yararlı Veri Boyu: IPv6 başlığının arkasındaki yararlı veri yükünün uzunluğunu belirtir. 16 bit uzunluğundadır. En fazla 65,535 Byte'lık veri büyüklüğünü işaret edebilir. Bu değerden büyük verilerin taşınması durumunda bu değer 0 yapılır ve düğümden-düğüme atlama başlığı, seçenek alanında "Jumbo-Veriyükü" özelliği işaret edilmek suretiyle temel başlığın arkasına eklenir.

Sonraki Başlık: 8 bit uzunluğundadır. Temel başlığın arkasına eklenmek suretiyle kullanılacak olan bir sonraki ek-başlığın tür bilgisi bu alanda taşınır.

Atlama Limiti: 8 bit uzunluğundadır. IPv6 paketinin yok edilmeden önce üzerinden geçebileceği düğüm sayısını işaret eder. IPv4 başlığındaki TTL değeri gibidir. Buradaki değerin 0 olması durumunda paket yok edilir ve paketin kaynak adresine ICMPv6 Zaman Aşımı mesajı gönderilir.

Gönderici Adresi: 128 bit uzunluğundadır. Paketin kaynak adresi bilgisi bu alanda taşınır.

Alıcı Adresi: 128 bit uzunluğundadır. Paketin ulaşması istenen hedefin adres bilgisi bu alan içerisinde taşınır.

3. IPv6/Yeni Nesil İnternet Protokolü Adresleme Yapısı

IPv6'da adresler genel olarak heksadecimal (16'lık tabanda) gösterilmektedir. IPv4'de 32 bit olan adres uzunluğu ise yeni protokolde 128 bit'e çıkarılmıştır. Bu şekilde $3{,}4x10^{38}$ civarında adresleme yapılabilmektedir. Adres gösterimi ise aşağıdaki gibi olmaktadır:

```
1234:5678:9ABC:DEF0:1234:5678:9ABC:DEF0
```

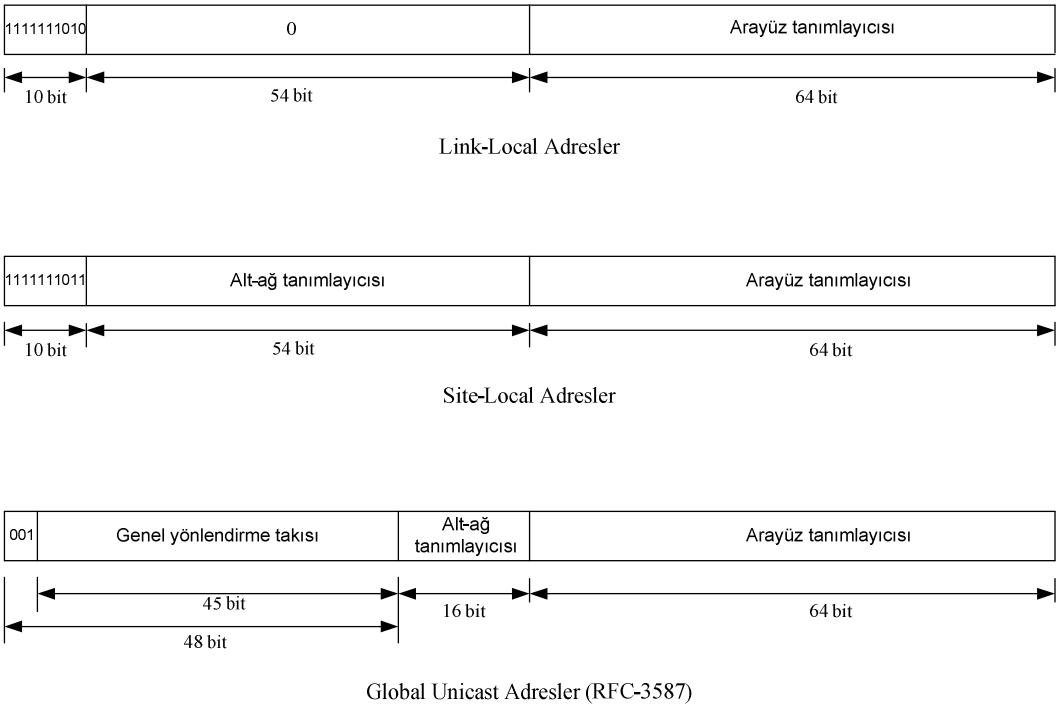
Görüldüğü gibi her dört karakterden oluşan gruplar birbirlerinden ":" karakteriyle ayrılmıştır. Yeni nesil protokolde adresleme şeklinin yanı sıra adres türü ve iletişim şekillerinde de değişiklik gözlenmektedir. Günümüzde yaygın şekilde kullanılan ve ağ uzmanları için bazı sorunları da beraberinde getiren yayın (broadcast) türü iletişim şekli yeni nesil İnternet Protokolünde kaldırılmıştır. Bu bağlamda yeni protokolde iletişim türlerine bakılacak olunursa [13] :

a) **Tek alıcılı** (unicast) : Bir düğümün bir arayüzünü gösterir. Aynı arayüz birden fazla adrese sahip olabilir. Örneğin iki farklı İnternet erişim sunucusuna bağlı bir abonenin her iki erişim sunucusundan görünen adresleri birbirinden farklıdır.

b) **Herhangi bir alıcılı** (anycast) : Birden çok arayüzü (bunlar farklı düğümlere ilişkin olabilir) belirten bir adrestir. Bu adrese gönderilen bir paket bu adrese sahip arayüzlerden en yakındakine teslim edilir.

c) **Çoklu-alıcılı** (multicast) : Birden çok arayüzü belirten bir adrestir. Bu adrese gönderilen bir paket bu adrese sahip arayüzlerin hepsine teslim edilir.

Yukarıda sözü edilen trafik şekilleri dışında ağ cihazımızın alabileceği adres sınıfları da, IPv6 ile birlikte, şu şekilde olmaktadır [14]:



Şekil 3. IPv6'da Adres Sınıfları

- **Global adresler**: Günümüzde genel olarak İnternet'te kullandığımız adresler olarak niteleyebiliriz. Bu adresler İnternet ortamında yönlendirilebilir ve ulaşılabilir. IANA tarafından ayrılmış ve RFC-3587'de tanımlanmış olan Global *unicast* adreslerde en anlamlı ilk 3 bit "001" olmaktadır. Bundan sonraki ilk 45 bit genel (global) yönlendirme takısı için ayrılmıştır. Sonraki 16 bit alt ağ tanımlayıcısı ve kalan 64 bit arayüz tanımlayıcısı için ayrılmıştır.

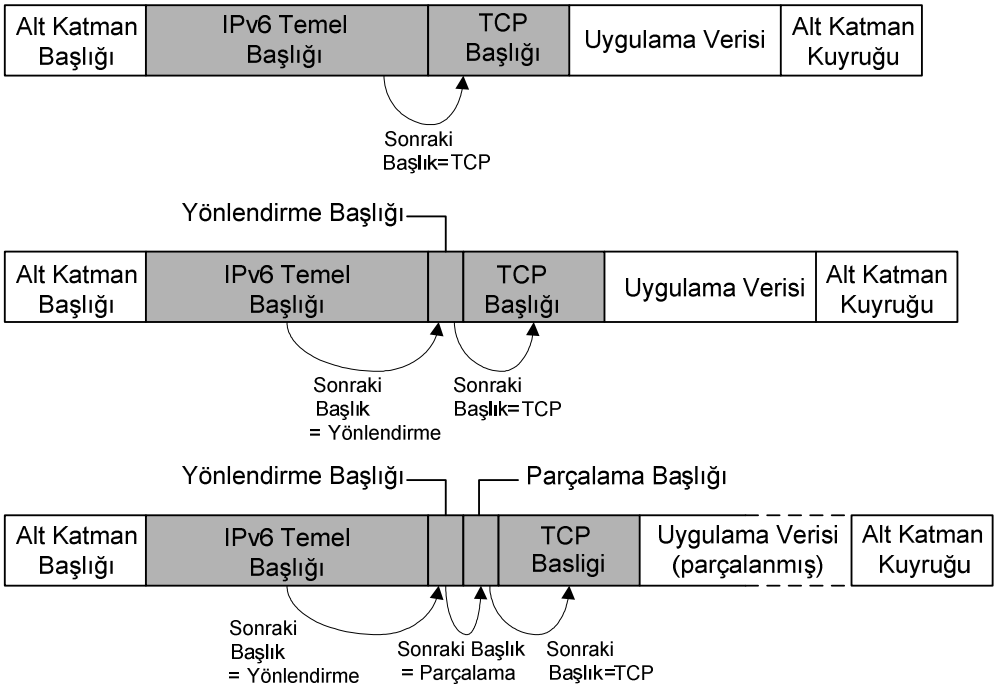
- **Link-local adresler**: Aynı bağlantı üzerindeki komşu düğümlerle iletişimde kullanılacak adreslerdir. Yönlendiriciler bu türdeki trafiği hat (link) dışına iletmezler. Link-local unicast adreslerde en anlamlı 10 bit "1111 1110 10" şeklindedir. Sonraki 54 bit "0" dır. Kalan 64 bit arayüz tanımlayıcısını içerir.

- **Site-local adresler**: Aynı organizasyon (site) içerisinde kullanılacak adreslerdir. Bunu günümüzde işyerimizin ağı içerisinde veya evde kullandığımız adreslere

benzetebiliriz. Bu türdeki trafik yönlendiriciler tarafından organizasyon içerisinde kalacak şekilde yönlendirilebilir. Site dışına çıkan paketler yönlendiricilerden geçemez. *Site-local unicast* adreslerde en anlamlı 10 biti "1111 1110 11", sonraki 54 bit alt ağ tanımlayıcısını kalan 64 bit ise arayüz tanımlayıcısını içerir.

4. IPv6'nın Ek Başlıkları

IPv6'nın getirdiği en büyük değişimlerden birisi ise ek-başlık (extension header) yapısıdır. Temel IP başlığına ek olarak bu alan içerisindeki "sonraki başlık" (next header) kısmı sayesinde ilave edilmek istenen ve değişik özellikleri barındıran ek-başlıklar, IP başlığına ilave edilebilir.



Şekil 4. IPv6 Ek-Başlık Kullanımı

Eğer ek-başlık kullanılacaksa, geçerli başlık içerisindeki "sonraki başlık" kısmına, eklenmek istenen ek-başlığın kodu girilmelidir. Bkz. RFC-1700

Örneğin: 0-Düğümde-düğüme atlama başlığı

6-TCP

17-UDP

41-Paketlemeli yönlendirme başlığı

43-Yönlendirme başlığı

44-Parçalama başlığı.

Bunlar ilk olarak RFC-1883 ile tanımlanmışlardır. Şu andaki güncel olan standart ise RFC-2460'dır. Ek-başlıkların bu standart tarafından önerilen kullanım sırası şu şekildedir:

- IPv6 temel başlığı
- Düğümden-düğüme atlama başlığı (Hop-by-Hop Options header)
- Alıcı/hedef başlığı (Destination Options header)
- Yönlendirme başlığı (Routing header)
- Parçalama başlığı (Fragment header)
- Doğrulama başlığı (Authentication header)
- Emanet verinin paketlenmesi başlığı (Encapsulating Security Payload header)
- Alıcı/hedef başlığı (Destination Options header)
- Üst katman başlığı

Bu başlıklardan birisi hariç diğerleri yalnızca birer kez kullanılabilir. Sadece alıcı/hedef başlığı iki defa kullanılabilir (Birisi yönlendirme başlığından önce, diğeri üst

katman başlığından önce). Her ek-başlık 8-Byte'lık parçalar halinde kullanılmalıdır. Bu büyüklüğe tamamlanamıyorsa gerekli yerlere boşluk-doldurma işlemi yapılır.

Ek-başlıklar ve temel özellikleri kısaca aşağıdaki gibi özetlenebilir:

4.1. Düğümden-Düğüme Atlama Ek-Başlığı:

Şekil 5. Düğümden-Düğüme Atlama Ek-Başlığı

Düğümden-düğüme atlama ek başlığı paketin alıcısına giderken ara düğümlerde kullanılacak kontrol bilgilerini taşımak için kullanılır. Bu ek-başlık kullanılacağı zaman IPv6 temel başlığının ardına eklenmelidir. "Sonraki başlık" değeri 0'dır. Bu başlık içerisinde sırasıyla şu alanlar vardır:

Sonraki Başlık: 8 bit uzunluğundadır ve kendisinden sonra gelecek ek-başlığının tür bilgisini içerir.

Başlık Genişleme Uzunluğu: 8 bit uzunluğundadır. Düğümden-düğüme atlama başlığının kaç adet 8-sekizli (octets) gruptan oluştuğunu belirtir. İlk 8-sekizli bu hesaba dahil edilmez.

Seçenek Alanı: Değişken uzunluktadır. Bu alan için tanımlanmış 4 değer vardır.

Seçenek değeri:

— 0 ise tek Byte'lık doldurma işlemini;

— 1 ise 2 veya daha fazla Byte'lık doldurma işlemini;

— 5 ise yönlendirici uyarı seçeneğini (router alert option) ifade eder. (Belirli bir hedefe gönderilen bilgi datagramının, yol üzerindeki yönlendiricilerde özel değerlendirmeye tabii tutulmasın istendiği durumda kullanılır.)

— 194 ise Jumbo-Veriyükü'nü ifade eder. Jumbo-Veriyükü seçeneği ile 4.294.967.295 Byte'lık veriyükü taşınabilir.

Düğümden düğüme atlama başlığı aradaki tüm düğümler tarafından incelenen tek başlıktır. Gönderen düğümün bu başlığı kullanmaması halinde aradaki herhangi bir düğüm bu başlığı pakete ekleyip paketi iletemez, sadece bu başlık içerisinde iletilen değer üzerinde oynama yapabilir.

4.2. Yönlendirme Ek-Başlığı:

Şekil 6. Yönlendirme Ek-Başlığı

Yönlendirme başlığı, paketin hedef düğüme ulaşırken üzerinden geçmesi düşünülen diğer düğümlerin adres bilgisini içerir. "Sonraki başlık" değeri 43'tür. Yönlendirme başlığının içerdiği alanlar sırasıyla şunlardır:

Sonraki Başlık: 8 bit uzunluğundadır. Bir sonraki başlığın tür bilgisini içerir.

Başlık Genişleme Uzunluğu: 8 bit uzunluğundadır. Yönlendirme başlığının kaç adet 8-sekizli gruptan oluştuğunu gösterir. İlk 8-sekizli(64 bit) bu değere dahil edilmez. Yönlendirme türü değerinin 0 olduğu durumda başlık genişleme uzunluğu değeri, başlık içerisinde listelenen adres sayısının iki katına eşittir.

Yönlendirme Türü: 8 bit uzunluğundadır. Belirli yönlendirme başlık biçimlerini ifade eder. Varsayılan değer 0'dır.

Kalan Segment: 8 bit uzunluğundadır. Paketin alıcı düğüme ulaşmadan önce geçmesi gereken düğüm sayısını gösterir.

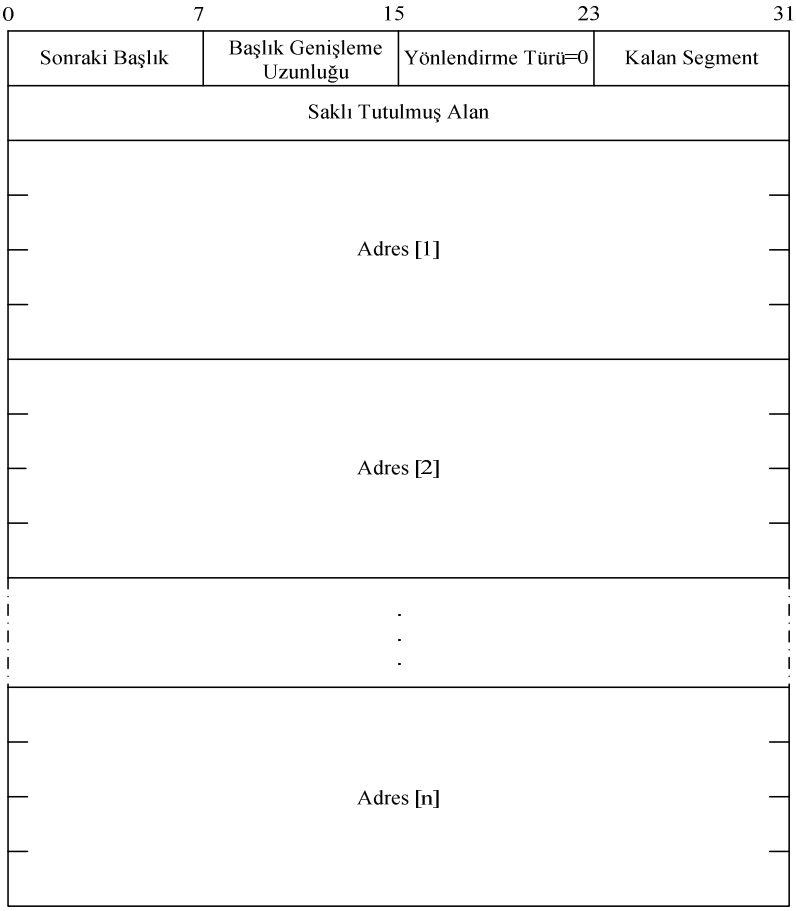
Türe Özel Veri: Yönlendirme Türüne bağlı olarak değişken uzunluktadır. Kalan segment alanından sonraki tüm kısmı kapsar.

Eğer, paket bir düğümde işlenirken, yönlendirme başlığının yönlendirme türü alanında tanımlanmamış bir bilgi varsa, işlem yapılmadan önce "kalan segment" alanına bakılır. Oradaki değere göre aşağıdaki işlemlerden biri gerçekleştirilir:

—Eğer kalan segment değeri sıfır ise, düğüm yönlendirme başlığını önemsemez, bu başlık içerisindeki sonraki başlık kısmında işaret edilen bir sonraki başlığa geçilir.

—Eğer kalan segment değeri sıfırdan farklı ise, düğüm paketi çöpe atar ve paketin kaynak adresi kısmındaki adrese ICMP Parametre Problemi, kod 0, tanınmayan yönlendirme türü hatasını işaret eden bir mesaj yollar.

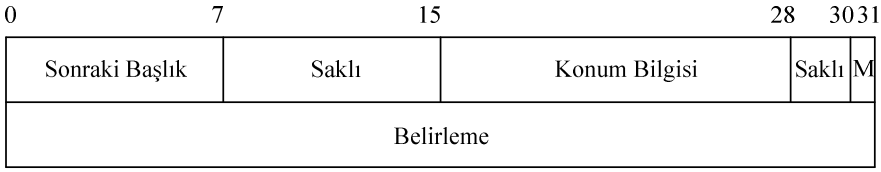
Yönlendirme Türü varsayılan 0 değerini aldığında örnek bir yönlendirme başlığı Şekil 7'deki gibi olmaktadır.



Şekil 7. Yönlendirme Türünün 0 Olması Durumunda Yönlendirme Ek-Başlığı

Eğer, düğüm yönlendirme ek-başlığını değerlendirdikten sonra, paketin gönderilmesi gereken yolun MTU (Maximum Transmission Unit) değerinin paketin boyundan küçük olduğunu tespit ederse, paketi çöpe atar ve paketin kaynak adresi kısmındaki adrese "paket çok büyük" ICMP mesajını gönderir.

4.3. Parçalama Ek-Başlığı:



Şekil 8. Parçalama Ek-Başlığı

Parçalama başlığı, kaynağın gönderdiği IPv6 paketi uzunluğunun, hedefe giderken geçtiği yolun MTU değerinden[1] daha büyük olması durumunda kullanılır. Bu özellik IPv4'te de olmakla birlikte, IPv6'daki fark parçalama işleminin sadece paketi gönderen kaynak tarafından yapılabilmesidir. "Sonraki başlık" değeri 44'tür. Parçalama başlığının yapısı incelenecek olursa içerdiği alanlar sırasıyla şunlardır:

Sonraki Başlık: 8 bit uzunluğundadır. Asıl paketteki parçalanabilir alandaki ilk başlık tür bilgisini içerir.

Saklı Tutulan Alan: 8 bit uzunluğundadır. İlerideki kullanımlar için saklı tutulmuştur. İletimde 0 değerini alır; alındığında ise önemsenmez.

Konum Bilgisi: 13 bit uzunluğundadır. Veri parçasının, orijinal paketteki parçalanabilir kısmın başından itibaren, 8-sekizlik gruplar halinde, kayıklık değerini verir. İlk parçanın değeri 0'dır.

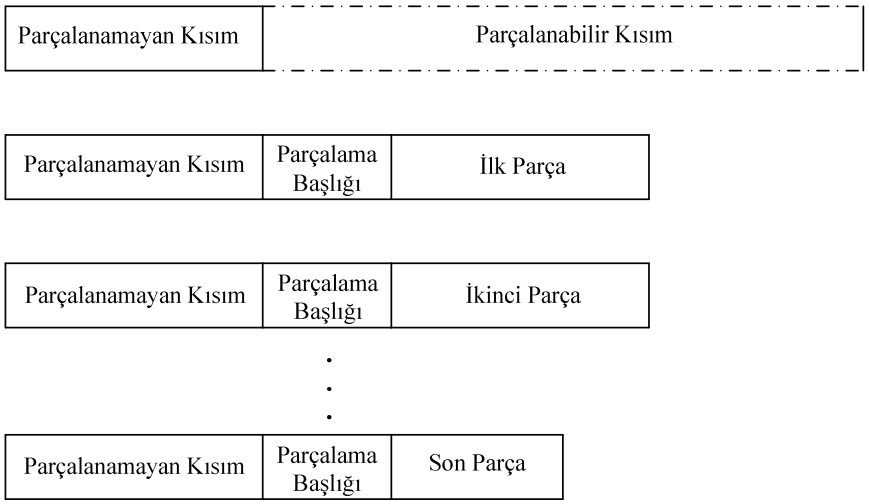
Saklı Tutulan Alan: 2 bit uzunluğundadır. Gelecekteki çeşitli ihtiyaçların karşılanması amacıyla saklı tutulmuştur. İletimde 0 değerini alır; alındığında ise önemsenmez.

M bayrağı: 1= Daha parçalanmış paket var; 0= Son parça.

[1] Bu değer "yol MTU keşfi" işlemi sonucunda belirlenir. Bu işlem kısaca düğümün iletişimde kullanacağı yol üzerinden, hata mesajı alınana kadar artan büyüklüklerde paket göndermesi, hata alındığında ise tuttuğu yol MTU değerini güncellenmesi şeklinde gerçekleştirilir. Daha ayrıntılı bilgi için bkz. RFC 1981.

Belirleme: 32 bit uzunluğundadır. Kaynak tarafından parçalanmış paketin her bölümüne bir belirleme değeri verilir. Bu değer bu alanda saklanır. Her belirleme değeri önceki gönderilen diğer parçalanmış paketlerdeki bölümlerin belirleme değerlerinden farklı olmalıdır.

Bir pakete parçalama işlemi uygulanması durumunda oluşan paketler şu şekilde gösterilebilir:



Şekil 9. Parçalama İşlemi

Orijinal veri iki kısma ayrılır. Parçalanabilen kısım ve parçalanamayan kısım. Parçalanamayan kısım IPv6 temel başlığı ve aradaki düğümlerde değerlendirilmesi gereken bazı ek başlıkları içermektedir. Yönlendirme başlığı, düğümden düğüme atlama başlığı, başka ek-başlık yok başlığı vb. gibi. Parçalanabilen kısım ise iletilecek veriyi ve hedef düğümde değerlendirilmesi söz konusu olan ek-başlıkları içermektedir. Parçalanabilir kısım 8-sekizlinin katları uzunluktadır. Parçalanmış paketlerin IPv6 temel başlığındaki veriyükü boyutu parçalanmış veriyi taşıyan paketin boyutunu gösterir. Parçalanmış paketlerin boyutu hedefe giden yolun MTU büyüklüğüne sığacak şekilde ayarlanmaktadır.

Yeniden birleştirme işleminde şu kurallar uygulanır:

- Yeniden birleştirilecek paketlerin kaynak ve hedef adresleri ile belirleme değerleri aynı olmalı.
- Parçalanamayan kısımdaki bölüm aynen alınır. Parçalanmış ilk veri paketinin(kayıklık değeri 0 olan başlığı içeren paket) parçalama başlığındaki "sonraki başlık" alanındaki değer, parçalanamayan paketin son başlığının içindeki ilgili alana atanır.
- Veri yükü değeri yeniden hesaplanır.

4.4. Alıcı/Hedef Ek-Başlığı:

Şekil 10. Alıcı/Hedef Ek-Başlığı

Alıcılarda değerlendirilmesi istenen ek bilgilerin taşınması için kullanılır. Ek-başlık sıralamasında iki kez kullanılabilen tek başlık budur. "Sonraki başlık " değeri 60'tır. Alıcı başlığının kullanımında iki yol vardır:

- Eğer yönlendirme başlığı kullanılmışsa, seçenek kısmı aradaki her hedef düğümde değerlendirilir.

- Seçenek kısmı hedefte değerlendirilir.

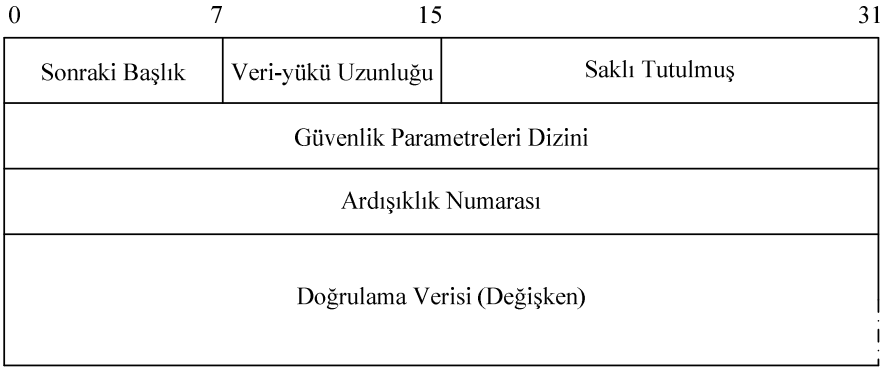
Alıcı başlığının içerdiği alanlar şunlardır:

Sonraki Başlık: 8 bit uzunluğundadır ve kendinden sonra gelecek ek-başlığın tür bilgisini içerir.

Başlık Genişleme Uzunluğu: 8 bit uzunluğundadır. Alıcı/Hedef başlığının kaç adet 8-sekizli gruptan oluştuğunu belirtir. İlk 8-sekizli bu hesaba dahil edilmez.

Seçenekler: 8-sekizlinin katları olacak şekilde değişken uzunluktadır. TLV Sıkıştırma[2] şeklinde kullanılan bir veya birkaç seçeneği içerebilir. RFC-2460'da bu alan için tanımlanmış "Pad1" ve "PadN" olmak üzere iki seçenek vardır.

4.5. Doğrulama Ek-Başlığı:



Şekil 11. Doğrulama Ek-Başlığı

Doğrulama başlığı taşınan paketin güvenliğine yönelik üç farklı unsura bünyesinde destek vermektedir:

Veri doğruluğu: Paketin asıl gönderici tarafından gönderilen paket olup olmadığının sınanması.

[2] TLV (Type-Length-Value) encoded: Ayrıntı için bknz. RFC 2460.

Veri bütünlüğü: Verinin iletim esnasında değiştirilip değiştirilmediğinin sınanması desteğini sağlar.

Yineleme engeli: Paketin yolda bir düğüm tarafından kopyalanıp içeriği değiştirilip tekrar iletilmesini engellenmesi.

Doğrulama başlığı yalnız kullanılabileceği gibi emanet verinin paketlenmesi (encapsulating security payload) başlığıyla birlikte de kullanılabilir. “Sonraki başlık” değeri 51’dir.

Doğrulama başlığının içindeki alanlar sırasıyla şunlardır:

Sonraki Başlık: 8 bit uzunluğundadır. Doğrulama başlığından sonra gelen veri yükünün türünü belirtir.

Veri-yükü Uzunluğu: 8 bit uzunluğundadır. Buradaki değer doğrulama alanının uzunluğunun 32 bit’in katı türünden karşılığının iki eksiğidir(Doğrulama başlığının ilk 8 sekizlisi sayılmaz.). Alabileceği en düşük değer 1’dir. Bu değer hata yakalama amaçlı kullanılabilir.

Saklı: 16 bit uzunluğundadır. Gelecekteki kullanımlar için saklı tutulmuştur. Günümüzde, bu başlığın kullanılması koşulunda bu alana 0 değeri verilmesi zorunlu kılınmıştır.

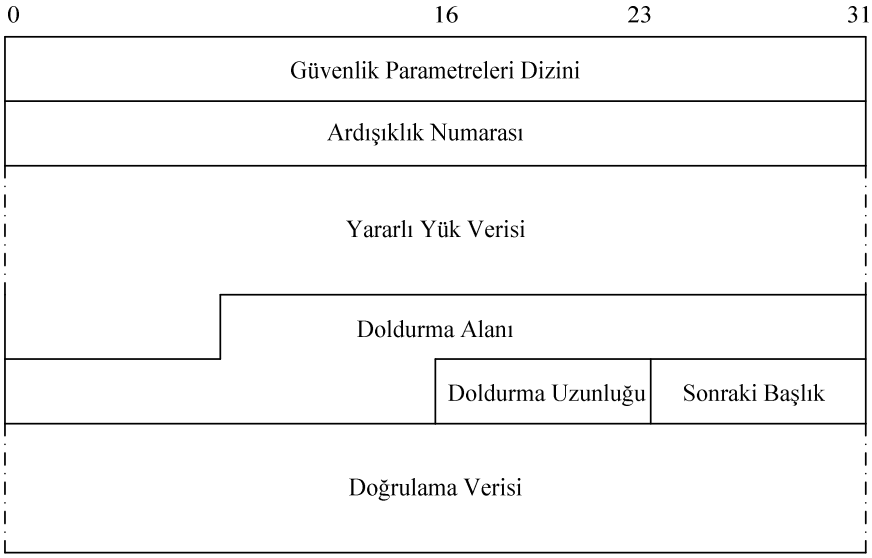
Güvenlik Parametreleri Dizini: 32 bit uzunluğundadır. Gönderen kimliğinin doğruluğunun kontrolü amaçlı kullanılır. IPSec güvenlik birliği (security association) desteği bu alanda verilmektedir. Standartta bu alan için 0 değerinin kullanılması önerilmiştir: Bu yerel (local) kullanımda hata tespiti amaçlı kullanılabilir. 1–255 arası değerler saklı tutulmuştur.

Ardışıklık Numarası: 32 bit uzunluğundadır. Monoton artan düzende sayaç değeri tutulur. Güvenlik birliği kurulduğunda alıcı ve gönderici düğümlerde bu sayaç

sıfırlanır. Buradaki değer hiçbir zaman bir döngüye girmez. Yeni bir güvenlik birliği kurulduğunda bu sayaç sıfırlanır. Bu işlem yineleme engelleme desteğini sağlar.

Doğrulama Verisi: Değişken uzunlukta olup 32 bit'in katları şeklinde artar. Bu alanda Bütünlük Kontrol Değeri (ICV) tutulur. Gerektiğinde doldurma işlemi yapılmalıdır. Bu alan veri bütünlüğü kontrolünün sağlanması için kullanılır.

4.6. Emanet Verinin Paketlenmesi Ek-Başlığı:



Şekil 12. Emanet Verinin Paketlenmesi Ek-Başlığı

Bu başlık, IPv4'de ve IPv6'da IPSec güvenlik servisine destek vermek amacıyla tasarlanmıştır. Bu başlık dört farklı unsura bünyesinde destek vermektedir. Bunlar:

Veri Gizliliği: Veri ele geçirilse bile içeriğinin, anlaşılamaması için çeşitli yöntemlerle gizlenmesi (örn. Şifreleme).

Veri Doğruluğu: Paketin asıl gönderici tarafından gönderilen paket olup olmadığının kontrolü.

Yineleme Engeli: Paketin yolda bir düğüm tarafından kopyalanıp tekrar iletilmesini engellenmesi.

Sınırlı Trafik Akış Gizliliği: Bu özelliğin kullanılması için tünel biçiminde iletişim seçilmiş olmalıdır. Bu şekilde daha etkili geçityolu (gateway) güvenliği sağlanmış olur.

Bu başlık tek başına kullanılabileceği gibi doğrulama başlığı ile birlikte veya iç içe biçimde (örn. tünellenmiş iletişim) kullanılabilir. Bu başlık için IPv6'da "sonraki başlık" değeri, IPv4'de de "protokol" kısmında ki değer 50 olmalıdır. Bu başlığın kullanılması durumunda, veri yapısı içerisindeki bazı alanların kullanılması zorunludur. Emanet verinin paketlenmesi başlığının veri yapısı şu şekildedir:

Güvenlik Parametreleri Dizini: 32 bit uzunluğundadır. Gönderici kimliğinin doğruluğunun kontrolü amaçlı kullanılır. IPSec güvenlik birliği (security association) desteği bu alanda verilmektedir. Standartta bu alan için 0 değerinin kullanılması önerilmiştir, bu yerel kullanımda hata tespiti amaçlı kullanılabilir. 1–255 arası değerler ise gelecekteki kullanımlar için saklı tutulmuştur. Bu alanın kullanılması zorunludur.

Ardışıklık Numarası: 32 bit uzunluğundadır. Monoton artan düzende sayaç değeri tutulur. Güvenlik birliği kurulduğunda alıcı ve gönderici düğümlerde bu sayaç sıfırlanır. Buradaki değer hiçbir zaman bir döngüye girmez. Yeni bir güvenlik birliği kurulduğunda bu sayaç sıfırlanır. Bu işlem yineleme engelleme desteğini sağlar. Bu alanın kullanılması zorunludur.

Yararlı Yük Verisi: Değişken uzunluktadır ve sonraki başlık alanında türü tanımlanmış veriyi içerir. Eğer kullanılacak şifreleme algoritması kriptografik senkronizasyon verisi gerektiriyorsa bu veri bu alanda taşınabilir. Bu alanın kullanılması zorunludur.

Doldurma (şifreleme için): 0–255 Byte uzunluğunda olabilir. Bu ek-başlık içerisinde kullanılması zorunlu olmamakla birlikte bütün uygulamaların bu kısmı desteklemesi ise zorunlu kılınmıştır. Kullanılabileceği bazı durumlar ilgili RFC'de açıklanmıştır.

Doldurma Uzunluğu: 8 bit uzunluğundadır. Bir önceki alanda ne kadar Byte'lık doldurma yapıldığının değeri tutulur. Bu alanın kullanılması zorunludur.

Sonraki Başlık: 8 bit uzunluğundadır. Emanet verinin paketlenmesi başlığından sonra gelecek olan başlığı gösterir. Bu alandaki değerler IPv4 protokol alanındaki değerler ile aynıdır. Bu alanın kullanılması zorunludur.

Doğrulama Verisi: Değişken uzunlukta olup emanet verinin paketlenmesi başlığının doğrulama verisi alanı haricinde olan kısmın bütünlük kontrol değerini içerir.

5. IPv6'nın Uygulamalara Etkisi ve Ulaştığımız Öngörüler

IPv6'nın uygulamalara etkisinin nasıl olacağı, bu yeni protokolün adres yapısı ve başlık yapısındaki ek-başlıkların incelenmesiyle ortaya çıkarılabilir. Acaba, ek başlıkların uygulamaya etkisi nasıl olacaktır? Bu konudaki çalışmanın sonucu olarak "elde ettiğimiz öngörüler" ek-başlık adları verilerek aşağıdaki gibi özetlenmiştir:[13]

5.1. Adresleme Yapısı ve Öngörülerimiz

▪ Düğümlerin iletişim ağına kablosuz erişir hale geleceği düşünülürse, mobil düğümlerde herhangi bir adres değişikliği yapılmadan ağa erişimi sağlanabilecek.

▪ Her arayüzün birden fazla adresi olması, dolayısıyla yeni programlarda bunun gözönüne alınması gerekecek. Günümüzde kullanılan güvenlik yazılımları tarafında da buna yönelik değişimlerin gözlenmesini beklemekteyiz. Örn: firewall yazılımlarında iletişimin dinlenmesi gibi.

▪ Yayın (broadcast) türü adreslemenin kaldırılması, onun görevini çoklu-gönderim adresleme yapısının gerçekleştirmesi dolayısıyla gereksiz trafik yükü ortadan kalkacaktır. Örneğin 1000 düğüme bir veri yollamak için belki de milyonlarca düğümde gereksiz trafik yaratılması engellenecek. Bu sayede ağ ortamlarında verimin daha da artması sağlanacaktır.

5.2. Düğümden-Düğüme Atlama Başlığı ve Öngürülerimiz

▪ Paketlerin göndericiden alıcısına giderken üzerinden geçtiği yönlendiricilere ayrı ayrı kontrol bilgisi iletmesi birçok uygulama için büyük esneklik sağlar; bu bir çeşit, yönlendiricileri "kaynaktan yönetmek gibi bir şeydir" denilebilir.

▪ Bu başlığın seçeneklerinden birisi olan jumbo veri-yükünün kullanılması ile büyük miktarda veri bir paketle iletilebilir.

5.3. Alıcı/Hedef Başlığı ve Öngörülerimiz

▪ Gönderilen verinin alıcıda nasıl değerlendirileceği bilgisinin bu başlık alanından gönderilebilmesi, gönderici ile alıcı arasında yönlendirme katmanı düzeyinde anlaşma yapılmasına olanak verir.

5.4. Yönlendirme Başlığı ve Öngörülerimiz

▪ Yol rotası verilerek aynı veriye ait paketlerin aynı güzergâhtan gitmesi birçok gerçek-zamanlı (real-time) uygulamaya destek sağlar. Böylece gerçek-zamanlı uygulamaları geliştirmek daha kolay olur. Sanki devre anahtarlamalı bir bağlantı şekli oluşturulmuş olunur. Dolayısıyla devre anahtarmalı sistemlerin olumlu yanlarından yararlanılmış olunur.

5.5. Parçalama Başlığı ve Öngörülerimiz

▪ Verinin iki uç arasında aktarılabilecek en büyük uzunlukta gönderilmesi bazı uygulamalarda yarar sağlar. Özellikle verinin birbiri ardı sıra değerlendirildiği uygulamalarda yararlıdır.

▪ Paketlerin yönlendiricilerde parçalanmaması onlardan ciddi sayılabilecek bir yük alır. Uygulama yazılımı tarafından paket parçalanması yönetilmeli ve yol MTU değerleri göz önüne alınmalıdır.

5.6. Doğrulama Başlığı ve Öngörülerimiz

▪ Gönderilen verinin gerçek göndericisinin bilinmesi ve bütünlüğünün sağlanması iş yaşamı için kaçınılmaz gereksinimdir. Böylesi gereksinimler büyük ölçüde sağlanacaktır.

▪ Yineleme engeli (anti-replay) ile "spoofing" ve "sniffing" türü saldırılara karşı doğal bir destek sağlanmış olur.

5.7. Emanet Verinin Paketlenmesi Başlığı ve Öngörülerimiz

▪ Günümüzdeki uygulamalarda 3'üncü katmandaki IP protokolünde şifreleme için destek yoktur. Örneğin güvenli bir iletişim için kullanılan şifreleme yöntemlerinde şifreler uygulama verisi olarak taşınıyordu. IPv6 ile bu işlem bu kısımdan alınmış ve IP başlığının içerisine yerleştirilmiştir. Böylece buradaki şifreleme bir veri olarak uygulama katmanına çıkarılmak yerine daha alt katmanlarda çözümlenerek uygulama katmanından soyutlanır, bu da güvenlik tarafında olumlu bir gelişmedir.

5.8. Sonuç ve Değerlendirme

IPv4'ün mimarisi gereği eksik kaldığı noktaları gidermesi, çare getirmesi için hedeflenen bir çalışma olarak sunulan IPv6 kuşkusuz bir süre sonra vazgeçilmez (defacto) bir yönlendirme protokolü olacaktır. Bu yeni protokolün uygulamalara etkisi onun adres yapısı ve başlık yapısındaki ek-başlıkların incelenmesiyle ortaya çıkarılabilir. Örneğin, gezgin kullanıcıların adreslerinde herhangi bir değişiklik yapılmadan erişim sağlanması; çoklu-gönderim adresleme yapısının gereksiz trafik yükünü ortadan kaldırması; yönlendiricilerin gelen paket üzerindeki davranışlarının kaynaktan denetlenebilmesi olanağı; büyük miktarda verinin bir paketle iletilebilmesi; yol rotası verilerek aynı veriye ait paketlerin aynı güzergahtan gitmesi; paketlerin yönlendiricilerde değil de gönderen

düğümde parçalanması; verinin gerçek göndericisinin bilinmesi ve bütünlüğünün sağlanması; yineleme engeli (anti-replay) ile "spoofing" ve "sniffing" türü saldırılara karşı doğal desteği gibi özellikleri uygulamaları daha etkin ve güvenilir çalışmaya yöneltecektir.

Bütün bunların yanı sıra IPv6 gelişime açık yapısı ile birçok ihtiyaca cevap verebilecek bir yönlendirme protokolüdür.[13]

6. Günümüzde İnternet'te Güvenlik

IPv6'nın güvenlik konusundaki avantaj ve dezavantajlarını görebilmek için herşeyden önce günümüzdeki mevcut İnternet altyapısında karşılaşılan saldırıları incelemek gerekmektedir. Günümüzde İnternet büyük bir hızla gelişmektedir. Korunmaya yönelik çeşitli güvenlik mekanizmaları da geliştirilmektedir. Fakat maalesef İnternet hala yeterince güvenli bir ortam değildir. Bu konu için gerek bilimsel dünyadan gerekse ticari kurumlar tarafından çalışmalar sürdürülmektedir. Bir verinin içeriğinin gizli kalması için şifreleme teknikleri ne kadar karmaşıklaştırılsa, şifre uzunlukları ne kadar arttırılsa diğer yandan teknolojik altyapı da hızla geliştirilmektedir. Günümüzde kullanıcılar 3GHz frekansta işlemci kullanabilmektedirler, son kullanıcılara daha yüksek hızla İnternet erişimi sağlanmaktadır ve İnternet aynı zamanda paralel çalışmalar için de kullanılabilmektedir. Dolayısıyla "hiçbir zaman tam güvenlik sağlanamaz" deyişi güvenlik uzmanlarının ortak fikri olmuştur. Fakat olası en yüksek düzeyde güvenliği sağlamak ise gerek ticari gerekse kişisel özel verilerimizin gizliliği açısından kritik bir gereklilik olmaktadır; gelecekte de olmaya devam edecektir. Günümüzde karşılaşılan saldırılar genel olarak şu şekilde sıralanmaktadır: [15]

- Keşif (reconnaissance)
- Başlıkta oynama ve parçalama işlemi (Header manipulation and fragmentation)
- 3. veya ve 4. katman seviyesinde aldatma (3. and 4. layer spoofing)
- ARP ve DHCP atakları (ARP and DHCP attacks)

- Yayınla saldırıya maruz bırakma (Broadcast amplification attacks-smurf)
- Yönlendirme atakları (Routing attacks)
- Paket gözleme (Sniffing)
- Uygulama katmanı saldırıları
- Sahte cihazlar
- Ortadaki adam saldırısı (Man in the middle)
- Paket seli (Flooding)

6.1.Keşif Atakları:

Bu ataklar bir saldırı şekli olmaktan çok, arkasından yapılacak saldırılar için, saldırganın hedef hakkında bilgi toplamasıdır. Saldırgan kurban durumundaki ağ hakkında mümkün olduğunca çok bilgi toplamalıdır. Bu, ağ araçları, arama motorları ve teknik doküman desteği kullanılarak yapılabilir. Bu amaçla kullanılan araçlar hedef cihaz ve/veya ağ hakkında yazılımsal ve donanımsal olarak önemli ipuçları vermektedirler. Bu, karşımızdaki cihazın kullandığı işletim sistemi olabileceği gibi, bunun bir bilgisayar olması halinde üzerinde çalışan uygulamalar, açık servisler ve açık portlar gibi bilgiler de olabilir. Bunların dışında saldırganın hedefindeki ağ yapısı hakkında çeşitli bilgilerde elde edilebilmektedir. Keşif ataklarına örnek olarak şunları verebiliriz:

- *Ping komutu*: Ping komutu iki uçbirim arasında 3. katman düzeyinde bir iletişimin kurulup kurulamadığına yönelik bir kontrol aracıdır. İki uçbirim arasında fiziksel bir bağlantı sağlanmışsa ve de bu uçbirimlerde IP protokol yığını düzgün olarak çalışmakta ise bize bir uçtan diğerine yolladığı kontrol paketinin istatistiksel değerlerini geri döndürür. Bir saldırgan bunu kurban ağın sınırlarını belirlemede ve ağı keşfetme aşamasında kullanabilir.

- *Port taraması*: Erişilebilir uçsistemler keşfedildikten sonra saldırgan bu sistemlerde 4. katman düzeyinde açık olan portları taramak suretiyle erişilebilen ve aktif olan servisleri öğrenebilir.

- *Uygulama ve açık taraması*: Uçsistem cihazında çalışan uygulamalarda var olan açıklar günümüzde en popüler tehditlerden biridir. Bu, uçsistemdeki bir işletim sistemi veya Web-sunucusu uygulaması olabileceği gibi yönlendirici, geçit yolu ve ateş duvarı gibi cihazlardaki yazılımlar da olabilir. Saldırgan hedefteki sistemde çalışan yazılımları ve bunların açıklarını taramak suretiyle sistem hakkında daha detaylı bilgiye erişmiş olur.

6.2. Başlıkta Oynama ve Parçalama İşlemi:

Bir diğer saldırı tekniği de paket parçalama işlemi ve başlık üzerinde yapılan diğer oynama işlemleriyle gerçekleştirilen saldırılardır. Bu ataklar genel itibariyle iki amaca yöneliktir. Bunlardan ilki ağdaki güvenlik sağlayan donanımları aşmak, bir diğeri ise direk ağ yapısına yönelik olmaktadır. Paket parçalama işlemi, paketin, maksimum iletilebilecek paket boyutu (MTU) değerinin, paket boyutundan küçük olduğu yollardan iletilebilmesi için parçalara ayrılması ve alıcıda bu parçaların tekrar birleştirilmesi işlemidir. Fakat bu yöntem günümüzde bir saldırgan tarafından, saldırıda bulunacağı hedefe ulaşabilmek için aradaki güvenlik cihazlarını aşmasına da alet edilebilir. Günümüzde kullanılan güvenlik cihazları ve yazılımları hedefe iletilmek üzere kendilerine gelen paketi belli kriterlere göre inceleyip tehdit unsuru bir veri görmemeleri durumunda alıcıya iletirler. Saldırganın gönderdiği paketteki zararlı veri normal şartlarda güvenlik cihazı tarafından engellenebilecekken, bu paketin parçalanarak gönderilmesi durumunda ise, aradaki güvenlik yazılımı gelen kötü amaçlı verinin sadece bir parçasını görüp, bunun bir tehdit unsuru olmadığına karar verip alıcıya gönderecektir. Saldırgan bu şekilde aradaki güvenliği saf dışı etmiş olur. Bu veri alıcıda tekrar birleştirildikten sonra işleme sokulur ve saldırgan amacına ulaşmış olur.

Bu saldırıya yönelik bir çözüm olarak güvenliğe yönelik cihaz ve yazılımlarda alınan parçalanmış paketlerin bütün parçalarının bir tampon bellekte tutulup daha sonra incelenmesi ve tehdit içermiyorsa alıcıya gönderilmesi yöntemi kullanılmaktadır. Fakat bu, büyük ağlarda trafiğin yavaşlamasına da sebep olmasından dolayı kimi zaman tercih edilmemektedir.

Paket parçalaması ve diğer türdeki başlık üzerinde oynama işlemlerinin kullanıldığı diğer saldırı yönteminde ise amaç çok sayıda parçalanmış paket kullanılarak bir ağdaki trafiğin yavaşlatılmasıdır.

6.3. Aldatma (Spoofing) Saldırıları:

Uçbirimlerin birbirlerine gönderdikleri paketlerde hedef-alıcı adresi ve portu bilgisinin yanı sıra gönderen uçbirimin adresi ve gönderildiği port numarası bilgisi de taşınmaktadır. Günümüzde en sık kullanılan saldırılardan biri de "IP spoofing" yani sahte adres kullanma işlemidir. Bu basitçe bir kullanıcının kendi adresini gizlemesi olarak düşünülebilir; fakat, diğer taraftan hedefteki makine aldığı veri paketlerine karşılık yolladığı cevap paketlerini bu sahte adreslere göndereceği için bunu masum bir adres gizleme olarak düşünmek yanlış olacaktır. Özellikle, sahte adresli birçok paketin hedefe ulaşması durumunda, hedef uçbirim de, birçok yanlış veya ulaşamayacağı adrese cevap paketleri yollayacak ve bu da hedef uçbirimin kaynaklarının daha uzun bir süre boşuna harcanmasıyla sonuçlanacaktır. 4'üncü katmanda aldatma atağında ise saldırganın amacı, hedef sistemde kurulan bir oturumun bir kopyasını kendisinde yaratıp oturumu ele geçirmesi veya uzak sisteme erişebilen yetkili adresi kendi adresi gibi göstererek ulaşmak istediği sistemle arasında bir oturum başlatmasıdır. Bu yöntemin esası sıra numarası tahmini ve IP aldatması işleminin birlikte kullanılmasıdır. Saldırganın yetkili konumundaki uçbirim ile erişmek istediği sistem arasındaki trafiği dinleyebilmesi veya ortadaki adam saldırısı yapabilmesi durumlarında oturum çalma işlemi çok daha kolay hale gelebilir.

6.4. ARP ve DHCP Atakları:

DHCP bir uçbirimin geçerli olan ağa erişip bu ağ üzerinden veri alış-verişini gerçekleştirebilmesi için gerekli olan parametrelerin, bu uçbirime sağlanması için geliştirilmiş bir protokoldür. Bu işlemi ağa bağlı olan DHCP sunucu gerçekleştirir. Uçbirimlere bildirilen parametreler ise uçbirime kullanması için IP adresi, kullanacağı ağın alt ağ (subnet) maskesi, dış ağlara çıkışta kullanacağı varsayılan geçityolu, isim çözümlemede kullanacağı DNS sunucu adresi gibi bilgilerden oluşmaktadır. Bu yönteme saldırı tarafından bakılacak olunursa, bir saldırgan ağa yetkiliymiş gibi çalışacak sahte bir DHCP sunucusu yerleştirip bu sunucunun istemcilere daha önce saldırgan tarafından belirlenmiş bilgileri parametre olarak bildirmesi sağlanabilir. Böylece saldırgan ağdaki uçbirimlerin trafiğini kendinin erişebileceği cihazlar üzerinden geçirip ağdaki trafiği izleyebilir.

Bir diğer teknoloji de ARP'dir. ARP, adres çözümleme protokolü olarak tanımlanmıştır. Uçbirimlerin kullandıkları ağ kartlarının kendilerine ait tekil MAC adresleri vardır. Yerel ağ içerisindeki iletişim gerçekte 2. katman düzeyindeki MAC adresleri kullanılarak yapılır. Fakat uygulamalar ve kullanıcı tarafında iletişim 3. katmandaki IP adresleri ile yapılıyormuş gibi görünmektedir. Dolayısıyla uçbirimlerde MAC adresi-IP adresi dönüşümünün yapılması gerekmektedir. ARP protokolü bu işlemi gerçekleştirir. Bu yöntemin temelinde ise uçbirimlerin ağda kendi MAC adresi ve IP adresi bilgisini içeren veri paketlerini yayınlamaları ve bir uç birimin başka bir hedef uçbirim ile iletişim kurmadan önce hedef IP adresinin karşılığı MAC adresini soran bir sorgu paketini yayınlaması vardır. Bu yöntem saldırı açısından incelendiğinde ise, saldırgan ağa kendi IP adresi ve kendi MAC adresi yerine hedef cihazın MAC adresi bilgisini içeren ARP mesajları yayınlaması ve dolayısıyla hedef cihaza ulaşması gereken bilgileri kendi IP adresine gönderimini sağlaması şeklinde kullanılmaya açıktır.

6.5. Yayınla Saldırıya Maruz Bırakma:

İnternet dünyasında "smurf" adıyla anılan saldırı çeşididir [23]. Hizmet durdurma saldırısının (DoS) bir türevidir. Bu saldırıda saldırgan bir ağa echo-istek mesajı gönderir; fakat kaynak adresi olarak saldırının hedefi konumundaki cihazın IP adresini kullanır. Böylece echo-istek (echo-request) yayın mesajını alan tüm uçbirimler buna karşılık olarak yolladıkları echo-yanıt (echo-reply) mesajını saldırının hedefindeki cihaza yollarlar. Böylece saldırgan hedef cihazda bir anda büyük bir trafik yaratıp hizmet dışı kalmasını sağlayabilir.

6.6. Yönlendirme Saldırıları:

Bu saldırı yönteminin amacı hedef ağdaki trafiği bozmak veya tekrar yönlendirmektir. Bunun gerçekleştirilmesi için birçok yol vardır. Bu atakta kullanılan teknikler kullanılan protokole göre değişir. Günümüzde kullanılan yönlendirme protokollerinin çoğunda yönlendiriciler arasındaki duyuru işlemleri için şifrelenmiş kimlik doğrulama yapılır. Uygulamada en çok önceden tanımlanmış anahtar ve MD5 kimlik doğrulaması kullanılır. [15]

6.7. Paket Gözleme (Sniffing):

Paket gözleme genel anlamda ağdaki gidip gelen veri paketlerinin içeriğinin gözlenmesidir. Saldırgan bu şekilde ağ üzerinde aktarılan önemli bilgilere erişmeye çalışabilir. Bunlar sisteme erişim şifreleri ve kullanıcıların kredi kartı bilgileri gibi kişinin özel bilgileri de olabilir.

6.8. Uygulama Katmanı Saldırıları:

Bu tanımlama OSI referans modelinin 7'nci katmanı olan uygulama katmanında gerçekleştirilen her türlü saldırıyı kapsamaktadır. Günümüzde İnternet'te yaşanan en yoğun saldırıların başında gelmektedir ve günümüzde İnternet'in güvenli olamamasının temel nedeni olarak da gösterilebilir. Genel bellek taşması saldırıları, Web uygulamalarına

yönelik ataklar (CGI atakları gibi), SQL-injection diye tabir edilen SQL komutlarının normal şartlarda kullanılmaması gereken yerlerde kullanılması yoluyla yapılan ataklar, virüsler ve solucanlar (worm) bu kategoriye girmektedirler. Virüs ve solucanlar günümüzde İnternet'in en büyük sorunlarından ikisidir. Gün geçtikçe İnternet'te yayılan virüs ve solucan oranı artmaktadır. Solucanlar bir ağda kendi kendine yayılabilen virüslerdir ve ciddi bir tehdit oluşturmaktadırlar. Bunlara örnek olarak Sapphire/Slammer solucanı gösterilebilir.

Şimdiye kadar yayılan en hızlı solucan olarak tanınmaktadır. Etkin olduğunda her 8,5 saniyede bir yayılma oranı iki katına çıkmıştır ve 10 dakika içerisinde hedeflediği açığına sahip sistemlerin %90'ına bulaşmış olduğu tahmin edilmektedir. Bu solucan Microsoft SQL Server ve Microsoft SQL Server Desktop Engine 2000 (MSDE2000) sistemlerindeki bir açık sayesinde hafıza taşması gerçekleştirebilmekte ve bu sayede kendini başka sistemlere gönderip yayılmasını sağlamaktadır. 75.000 civarı uçsistemin bu solucandan etkilendiği düşünülmektedir. Bu rakam az gibi görünse de havaalanlarındaki bilgisayarlara kadar birçok kamu kuruluşunun bilgisayarı bu saldırıdan etkilenmiştir. [24]

Bir diğer sorun ise "spam mail" olarak bilinen, alıcıların istemleri dışında aldıkları, genellikle ticari ilan ve duyuru içeren maillerdir. Bu mailler gereksiz yere yarattıkları trafik yüzünden toplam İnternet performansında düşüşe neden olmaktadırlar.

6.9. Ortadaki Adam Saldırısı (Man-in-the-Middle):

Temelde aldatma saldırısının kullanıldığı bu yöntemde saldırgan, bulunduğu ağdaki hedef cihaz ile hedefin iletişimde bulunduğu başka bir cihaz arasındaki trafiği kendi üzerinden geçirir. Bunu gerçekleştirebilmek içinse iki tarafa da gönderici IP adresi olarak birbirlerinin adreslerini fakat MAC adresi olarak kendi adresini içeren sahte ARP mesajları yollar. Uçbirimler gelen bu ARP paketi sonucunda ARP geçici belleklerini güncellerler. Böylece bir uçbirim diğerine bir paket yolladığında bu paket aradaki saldırgana, oradan da hedef uçbirime iletilir.

6.10. Sahte Cihaz:

Bu saldırı yöntemi basitçe, bir ağa fiziksel anlamda yetkisiz bir cihazın bağlanması ile gerçekleştirilmektedir. Bu bir taşınabilir bilgisayar, kablosuz ağ cihazı, erişim noktası, DHCP veya DNS sunucusu vs. olabilir.

6.11. Paket Seli (Flooding):

Bu saldırı yönteminde saldırgan hedefe doğru çok sayıda saldırı paketi gönderir. Buna ek olarak kendi adresini sahte bir adres olarak da kullanabilir (spoofing). Bu durumda saldırının kaynağını tespit etmek oldukça zorlaşır. Yerel veya dağıtık servis engelleme saldırıları (DoS), hedefin band genişliğini veya sistem kaynaklarını dolduracak kadar çok sayıda paket yollaması ile gerçekleştirilmektedir.

7. IPv6 Paket Yapısı Göz Önüne Alındığında Bu Saldırıların Geleceği Nasıldır?

Günümüzde yaygın olarak karşılaşılan İnternet üzerinden saldırı çeşitleri yukarıda açıklanmıştır. Peki, bu saldırılar gelecekte nasıl bir hal alacaklar? IPv6 bu saldırıların engellenmesi veya son bulması noktasında bizlere nasıl bir çözüm sunabilecek? Bu noktada çalışmalarım esnasında gördüğüm, araştırmacıların güvenlik noktasından ziyade diğer alanlarda IPv6 teknolojisiyle daha çok uğraştıklarıydı. Araştırmalarım esnasında gördüğüm, IPv6'nın güvenlik anlamında getirisi kimi makalelerde neredeyse güvenlik konusunda birçok sorunun ortadan kalkacağı gibi bir izlenim uyandırırken, bazı makaleler aslında durumun gerçek içyüzünü daha iyi yansıtmakta olduğudur. Bazı araştırmacı/yazarlar IPSec sayesinde IPv6'nın bir kurtarıcı olacağı gibi öngörülerde bulunsa da asıl gerçek; IPSec'in protokol ve uygulama bazında bazı açıklar içerip içermediği ve IPv6'nın uygulamaya geçilmesiyle birlikte IPSec'in ne derecede yaygın bir kullanımının olacağıdır. IPv6'nın uygulanmaya geçişiyle birlikte yukarıda bahsedilen tehditler açısından beklentiler şu şekilde olmaktadır:[15]

7.1. Keşif Atakları

- Adres çokluğundan dolayı port tarama işlemi zorlaşacaktır. IPv4'de varsayılan alt ağ büyüklüğü 2^8 iken IPv6'da varsayılan alt ağ büyüklüğü 2^{64} olmaktadır. Bir alt ağ içerisinde çok fazla sayıda adres kullanabileceğimizi düşünürsek bu ağ üzerinde düğüm veya uçbirim arama işlemi bugünkü mimariye göre çok daha uzun bir süre alacaktır.

- TCP katmanında değişiklik olmadığından dolayı port tarama işleminde bir değişiklik olmayacaktır.

- Uygulama ve uygulama açıkları taraması ile ilgili bir değişiklik beklenmemektedir. Çünkü bunlar üst katman protokollerini ilgilendirmektedirler.

- IPv6 protokolünde multicast iletişim daha yaygın olacak ve bu iletişim türünü ağ içerisinde kullanan bazı önemli düğümlerin (yönlendirici ve NTP gibi) bulunması daha kolay olacaktır (yönlendirici keşif işlemi).

7.2. Başlıkta Oynama ve Parçalama İşlemi

- Sözce (string) imza denetimi konusunda IPv6'nın ek bir getirisi söz konusu olmamaktadır. Dolayısıyla bu tehditlere yönelik ağ yöneticilerinin kendi önlemlerini almamaları durumunda bu tehdit gelecekte de var olacaktır.

- RFC2460'da tanımlanan minimum MTU değeri 1280 oktet'dir. Bu noktada ağ yöneticilerinin minimum MTU değerinden düşük olan paketleri ağ cihazları üzerinden engellemesi tavsiye edilir. Eğer bu yapılmazsa söz konusu ağ'a birçok sayıda küçük paketle saldırı yapılması ve bunun sonucunda ağın trafiğinin oldukça yavaşlaması veya tamamen durması söz konusu olabilir.

7.3. Aldatma Saldırıları

- 4'üncü katmanda yapılan aldatma saldırısı ile oturum çalma işleminde bir değişiklik söz konusu olmamaktadır. Bu saldırının temeli düşünüldüğünde saldırıda suistimal edilen protokol esas olarak TCP protokolü ve bunun bünyesinde bulunan üç yollu el sıkışma tekniğidir. Yeni nesil İnternet Protokolü ile birlikte TCP protokolünde bir değişim öngörülmediğinden bu sorunun gelecekte de yaşanması beklenmektedir. Fakat IPSec desteğinin aktif bir şekilde yeni nesil protokolde kullanılması, kesin güvenlik sağlamamakla birlikte, optimum bir güvenlik seviyesinin sağlanmasını gerçekleştirebilecektir.

7.4. ARP ve DHCP Atakları

- IPv6'nın kendi doğasında DHCP veya ARP'yi güvenli kılacak bir özellik yoktur. Birçok durumda bağlantısız otomatik konfigürasyon özelliği ile DHCP'ye benzer bir hizmet sağlanabilmektedir. Günümüzdeki birçok işletim sistemi ile gelen DHCP sunucularında IPv6 desteği bulunmamaktadır. Yeni nesil DCHPv6 sunucularda DNS sunucusu, zaman sunucusu, IP telefon hizmeti sunucusu gibi ek konfigürasyon parametreleri hizmeti verilebilir. Dolayısıyla DHCP seviyesinde hala bir güvenlik ihtiyacı söz konusu olmaktadır. Maalesef bağlantısız oto konfigürasyon mesajları taklit edilebilir ve bu işlem cihaza erişilememesine neden olabilir. Bunu engellemeye yönelik yönlendirici-duyuru mesajı ile güvenilir bir port konsepti birlikte kullanılabilir.

- ARP açısından bakacak olursak, IPv6 da ARP'nin yerine yeni bir çözüm olan komşu keşfetme işlemi getirilmiştir. Bu güvenlik açısından ARP ile aynı seviyededir. Bu protokolde kullanılan komşu-duyuru ve keşfetme mesajları taklit edilebilir ve komşu keşfetme protokolünce kullanılan geçici bellekte olan bilginin üstüne yazılabilir. Buna örnek olarak taklit edilmiş bir yönlendirici keşfetme paketi içerisine sahte yönlendirici bilgisi yerleştirilebilir ve böylece uçbirimlerin trafiğinin

bu sahte yönlendirici üzerinden akması sağlanabilir. Bunun sonucunda da trafik bu yönlendiricide kayıt edilebilir.

- DHCPv6 ile ilgili güvenlik çalışmaları sürmektedir.

7.5. Yayınla Saldırıya Maruz Bırakma (Smurf)

- IPv6'da yayın türü trafik kaldırılmıştır ve saldırı riskini azaltmak için yeni bazı teknikler geliştirilmiştir. Örneğin hedef olarak multicast, link-layer multicast veya link-layer broadcast adresleri kullanan paketlere cevap verilmesi engellenmiştir.

7.6. Yönlendirme Atakları

- Birçok protokolün güvenlik mekanizması IPv4'den IPv6'ya geçişle birlikte henüz değişmemiştir. Domainler arası yönlendirme bilgilerinin taşınması için BGP protokolü kullanılmaya devam etmektedir. Bununla birlikte BGP protokolü TCP katmanında kimlik doğrulaması için MD5 kullanmaya devam etmektedir. OSPFv3 protokolünde kimlik doğrulama başlığı kaldırılmıştır. RIPng (Routing Information Protocol Next-Generation) protokolünde de kimlik doğrulama özelliği yoktur. Bu iki protokol bilgileri aktarırken güvenlik kısmında IPSec AH ve ESP başlıklarına güvenmektedirler. Dolayısıyla IPSec protokolünün güvenirliği bu noktada da önem taşımaktadır.

7.7. Paket Gözleme

- Trafiğin dinlenilmesi saldırısına karşılık IPv6 protokolünün kendi içerisinde IPSec desteklemesi bir çözüm olarak gözükmektedir. Fakat IPSec ve güvenlik birliğinin kurulmasında kullanılan IKE ve ISAKMP protokolleri ayrı protokollerdir ve bunlar için geçerli güvenlik sorunları devam ettikçe IPv6'da da paket gözleme türü saldırıların gerçekleştirilebilmesi mümkün olacaktır.

7.8. Uygulama Katmanı Saldırıları

- Bu saldırılar İnternet Protokolü'nün uygulandığı ağ katmanına yönelik olmadığı için bu saldırıların aynen geçerli olması beklenmektedir. IPv6'nın kendi içerisinde IPSec desteklemesi aradaki iletişimin şifrelenmesine yönelik destek verecektir. Ancak bu, saldırıların kesilmesini sağlamaz. Bu tarz saldırılar şifrelenmiş kanallardan geçerek hedeflerine ulaşıp aynı zararı verebilirler. Fakat bunun getirisi olarak saldırının kaynağının keşfine yönelik geri izleme işlemi daha kolaylaşacaktır. Yeni nesil protokolün de IPSec desteklemesi ile birlikte uç cihazlarda bu protokol uygulanırsa güvenlik gereksinimleri biraz daha azalacaktır çünkü firewall veya IDS'ler şifreli trafiği görmektedirler fakat içeriğini okuyamadıkları için veri hakkında karar verememektedirler.

7.9. Sahte Cihazlar

- Bu saldırı IPv4 sistemlerde oldukça kullanılmaktadır ve maalesef IPv6'da yeterince değişmemiştir. Eğer IPSec IPv6'da daha çok yönlü bir şekilde kullanılırsa cihaz doğrulanması ile ilgili saldırıların önemli ölçüde azalması beklenmektedir.

7.10. Ortadaki Adam Saldırısı

- IPv6'nın bu saldırıya karşı etkinliği tamamen IPSec protokol kümesinin, özellikle de IKE protokolünün zaafları oranında olabilmektedir. Bilindiği üzere IPSec uygulanmadığı durumda IPv6'nın bu tarz bir saldırıda IPv4'den farkı olmamaktadır. Bu saldırıya karşı etkinliği IPSec protokol kümesi sağlamaktadır fakat bu protokolün de çeşitli zaafları mevuttur.

7.11. Paket Seli Saldırısı

- Temel ilke olarak bu atak IPv6'da da değişmemektedir. Yerel veya dağıtık DoS saldırıları yine kaynakları tüketme yolunda en basit saldırılardan biri olma özelliğini

korumaktadırlar. Bu konuda saldırı tespiti ve geri izleme teknikleri IPv4'de olduğu gibi IPv6'da da uygulanabilmektedir.

Günümüzdeki saldırıların yeni nesil İnternet Protokolü'nün hayata geçirilmesi ile birlikte geleceğinin nasıl olacağına yönelik öne sürülen düşünceler bu şekildedir. Bütün bunların dışında tabii ki yeni tanımlanan paketler ve yeni protokol ile yeni saldırı türlerinin ortaya çıkması kuvvetle muhtemeldir. Bunlara yönelik ipuçlarını ek-başlıkları incelediğimizde görebiliriz. Bu çalışmamızda ek-başlıklar gerek paket yapısı gerekse kullanıma sundukları yeni fonksiyonlar açısından incelenmiştir. Bunların sonucunda ortaya attığımız bazı öngörüler Bölüm 8'de sunulmuştur.

8. Ek-Başlıklar ve Güvenlik Açısından Öne Sürülen Düşünceler

Çalışmalarımızda her ek-başlık ayrı ayrı ele alınarak olası açıklar ortaya çıkarılmış ve tartışılmıştır.

8.1.Düğümden-Düğüme Atlama Ek-Başlığı

- Jumbo veri yükü ifadesi 65,535 Byte'dan büyük olan paketleri işaret etmektedir. Eğer oluşturacağımız paket bu değerin altında bir büyüklüğe sahipse o zaman düğümden düğüme atlama başlığı içerisinde bu ifade kullanılmaz. Kullanıldığı takdirde ise göndereceğimiz veri paketi büyüklüğü 65,535 Byte'dan büyük olmalıdır. Peki, bu seçeneği işaretleyip oluşturduğumuz bir pakette veri büyüklüğü bu limit değerden küçük olursa bir sorun oluşur mu?

  *RFC-1883'de bu husus belirtilmiştir ve protokolün algoritması çerçevesince bu durum engellenmiştir. Böyle bir durumun ilk alıcıda tespit edilmesiyle alıcı, paketin kaynak adresine ilgili ICMP hata mesajını gönderir ve paketi yok eder.

- Çok büyük bir veriyi parçalanmış paketin bir parçası olarak hedef düğüme yollayabilir miyiz?

*RFC-1883'de jumbo veriyükü seçeneğinin kullanıldığı paketlerde parçalama başlığının kullanılamayacağı belirtilmiştir.

- Öneri: Sadece düğümden düğüme atlama başlığı dışında, diğer ek-başlıkların hiçbirisi geçtiği düğümlerin her biri tarafından işleme sokulmuyor. Bu kısım İnternet ortamında gerçekleştirilen saldırılar hakkında bir uyarı sistemi olarak kullanılabilir. Şöyle ki, bir uçbirim kendisine veya kendisi üzerinden bağlı olduğu ağa yönelik bir saldırı yapıldığını tespit ettiğinde iletişimde bulunduğu tüm uçbirimlere belli süre çerçevesinde gönderdiği paketlere düğümden düğüme atlama başlığını da ekler ve bu başlık içerisinde seçenekler alanında saldırı türü ve saldırıyı yapan kaynağın adres bilgisini diğer uçbirimlere iletir. Böylece diğer uçbirimlerinde saldırı yapan kaynak hakkında uyarılması sağlanmış olur.

- Düğümden düğüme atlama başlığı içerisinde tanımlanmış değer olan yönlendirme uyarı seçeneği, özellikle uygulamaya geçildiğinde band genişliği ihtiyacı daha fazla olan gerçek zamanlı uygulamalar için, yönlendiriciler üzerinde, band genişliği rezerve edilmesi için kullanılabilmektedir. Bu bir çeşit "bu paketin ihtiyacı daha fazla, ona göre pakete yol verin" demeye benzer ve bunun için geliştirilmiş protokol RSVP'dir (Resource ReSerVation Protocol). Bütün bunların ışığında ele alacağımız yönlendirme başlığındaki ping-pong saldırısında yönlendirici uyarı seçeneğini kullanmamız durumunda ping-pong saldırısının daha etkili olabileceğini düşünmekteyiz.

- Bu başlık içerisinde yönlendirici uyarı seçeneğinin kullanılması durumunda, normal trafikte, yönlendiricilerde ciddi sayılabilecek bir performans kaybı beklenmemektedir. Fakat hizmet durdurma saldırıları ve benzeri paket seli (flooding) ataklarında bu seçeneğin kullanılması ile yönlendiricilerde önemli sayılabilecek bir performans sorunu yaratılabilir diye düşünmekteyiz. RFC–2711 içerisinde "güvenlik hususu" bölümünde düşüncemiz desteklenmektedir.

8.2. Yönlendirme Ek-Başlığı

- Yönlendirme başlığında paketin yol boyunca üzerinden geçmesi istenen düğümler belirtilmektedir. Bu ara adresler kısmında, ara düğümlerden birinin adresi olarak multicast adres kullanılması bazı faydalar sağlayabilir. Örneğin kötü niyetli biri uzaktaki bir ağın içyapısını keşfetmek amaçlı olarak komşu keşfetme veya yönlendirici keşfetme ICMP paketini yönlendirme başlığı ile birlikte kullanıp hedefe yollayabilir.

  * Bu düşünce çürümüştür: Yönlendirme başlığı içerisindeki "routing type" alanı değerinin "0" olması durumunda bahsedilen ara düğümlerin adresleri bu başlığa eklenir. Fakat protokolün çalışma algoritması bazında routing type değerinin "0" olması durumunda bu alanda multicast adreslerin kullanılması engellenmiştir.[16]

- Yönlendirme başlığında kalan segment sayısı ile ara düğüm sayısının eşit olmama durumunda adres alanı içerisinde başka veriler saklanabilir. Örnek olarak kalan segment sayısı 2 fakat başlıkta eklenmiş ara düğüm adresi sayısı 3 olması durumunda 128 bit = 16 Byte büyüklüğünde bir alan içerisine başka bir veri yerleştirilebilir. Bu, bir sonraki başlık olarak kullanılacak başlık verisi de olabilir.

  *Bu düşünce çürümüştür: Yine protokol algoritması tarafından başlık içerisindeki kalan segment sayısı ile başlığa yerleştirilmiş ara düğüm adres sayısı kontrol edilmektedir. Ayrıca başka bir başlık bilgisinin bu alana yerleştirilmesi de mümkün değildir. Çünkü sonraki başlığa geçmek için yapılan öteleme ek-başlık uzunluğu kısmında gösterilen değer kadardır.

- DoS türü saldırıları engellemek için etkin yollar geliştirilmediği sürece IPv6 teknolojisinde de bu saldırılar devam edecektir. Hatta IPv6'nın getirisi olan yönlendirme başlığı aracılığıyla veri paketinin hedefe giderken kullanacağı yolun seçilmesi lüksü sayesinde saldırılar aynı ara düğümler üzerinden hedefe

yönlendirilebilir; böylece sadece 1 hedefe yönelik değil, belirtilen ara düğümlere de yönelik DoS saldırısı yapılmış olur.

- Yönlendirme başlığında kullanılan ara düğüm adreslerinden biri sahte adres olabilir. Bu durumda sahte adresten bir önceki düğüm, sahte adrese paketi yollamaya çalışacaktır. Özellikle bu adres, bu ara düğümün erişemeyeceği bir adres olması durumunda ara düğüm bir süre bekledikten sonra paketin kaynak adresine paket ulaşmadı hata ICMP paketi yollayacaktır. Bu durumda kaynak adresinin de sahte olması gönderilen iki paketin de alıcılarına ulaşmaması ve bekleme süresi boyunca bu ara düğümün kaynağının meşgul edilmesi anlamına gelecektir. Tek olarak hiçbir etkisi olmasını beklemediğimiz bu saldırı birçok düğümden dağıtık olarak bir hedefe uygulandığında hedefe zarar verebilir.

- Yönlendirme başlığının ve kullanımının tanımlandığı ilgili RFC dokümanlarında ara düğüm adresleriyle ilgili herhangi bir kontrol mekanizmasından bahsedilmemektedir. Dolayısıyla kaynaktan birkaç düğüm sonrasından itibaren sıralı bir şekilde sadece iki düğüm arasında paketlerin aktarılması sağlanabilir. Biz bu saldırıyı karşılıklı olarak paketin iki düğüm arasında gidip gelmesinden esinlenerek ping-pong saldırısı olarak adlandırdık. Bu saldırı ile ilgili detaylı açıklamamız ve öne sürdüğümüz çözüm algoritması 9. bölüm içerisinde tartışılmıştır.

- Ek-başlık içerisinde kullanılan adres sayısı ile ilgili bir kısıtlamadan yine ilgili RFC'ler de söz edilmemiştir. Bu ilk başta düşünüldüğünde potansiyel bir açık olarak kullanılabilir fikri oluşturmuştur. Fakat bir başka açıdan bakıldığında başlık uzunluğunun belirtildiği alanın izin verdiği ölçüde(2^8=256, 256x8-sekizli/16-sekizli=128) adres kullanılabilir. Bu ise, günümüzde izin verilebilen TTL değerleri ve uygulamalarda yaratabildikleri sorunlar düşünüldüğünde ciddi problemlere neden olacağını düşünmemekteyiz.

- İnternet üzerinden yapılabileceği düşünülen ataklar için sadece global adresler üzerinde koruma sağlanmamalı. Aynı şekilde link-local ve site-local adresler için de aynı güvenlik önlemleri alınmalıdır. Zira yönlendirme başlığında sadece multicast türü adresler engellenmiştir. Fakat link-local veya site-local türdeki adresler için bir engelleme söz konusu değildir. Örneğin bir firmanın üyesi olan bir uçbirimin global adresini yönlendirme başlığında ara düğüm adresi olarak belirtip, bir sonraki ara düğüm olarak bu cihazın link-local veya site-local adresi ve/veya bu linkler üzerinde ulaşmak istediğimiz başka bir uçbirimin adresini yazabilmemiz anlamına gelmektedir. Bu şekilde bir paket, bir düğümün global adresi üzerinden site veya link-local adresine, oradan da bu düğümün herhangi bir komşusuna ulaşabilir.

- Ek-başlıkların kullanımına yönelik ilgili RFC'de önerilen bir kullanım sırası bulunmaktadır. Fakat herhangi bir zorunluluk uygulanmamaktadır. Uygulamaya geçildiğinde bu sıralamaya uyulmaması durumumda ise çeşitli başka güvenlik risklerinin beraberinde gelmesi olasıdır.

- Bir organizasyon (site) içerisinde aynı MAC adresine sahip olan birden fazla uçbirim olması durumunda bu uçbirimlerin site-local ve global adresleri de aynı olacaktır. Bu adrese gelen bir paket bu uçbirimlere iletilecektir.

  *Bu düşünce çürümüştür: Yönlendiriciler MAC adreslerini ve IP adreslerini tablolarında tutarlar ve herhangi bir çakışmayı önlemek için kontrol ederler. Öne sürülen türde bir durum olduğunda ise çakışma oluşacaktır.

- Sahte adresli bir trafik yaratıyoruz. Hedefteki yönlendirici bu saldırıyı tespit ettiğinde bizim bağlantımızın çıkış noktasındaki yönlendiriciyi uyarır ve bu yönlendirici de bizim paketlerimizin dış ağ'a erişimini engeller. Bu fikir hakkında detaylı bilgi için yönlendirme protokolleri incelenmelidir.

- Teorik fikir (daha çok adreslemeyle bağlantılı): IPv6 yönlendirme ek-başlığının getirilerinden biri olarak da yönlendirmede çeşitli politikaların uygulanabileceği

öngörülmektedir [17][25]. Bu politikaya örnek olarak, IP adresinin içerisindeki arayüz tanımlayıcısının içerdiği üretici firma kodunun elde edilip buna yönelik yönlendirme politikasının uygulanması verilebilir. Bu bir avantaj olarak kullanılabilir fakat bu avantaj belli firmaların cihazlarındaki açıklara yönelik saldırılarda saldırganın işini kolaylaştırmaktadır. Böylece saldırgan bu cihazları daha kolay bir şekilde tespit edip amacını gerçekleştirebilir. Günümüzde bu tarz bir saldırı yapılmak istendiğinde istenilen üreticiye ait cihazların bulunması tamamen şans eseri olmaktadır çünkü IPv6'dakine benzer bir şekilde üretici firma kodu adres içerisinde kullanılmamaktadır.

8.3. Parçalama Ek-Başlığı

- Parçalama başlığı içerisindeki veri yolda değiştirilemez fakat okunabilir. Bu konuda bir engel bulunmamaktadır. Parçalama işlemi kullanılarak yapılan bazı aradaki güvenlik cihazını atlatma saldırıları ileride de geçerliliğini koruyacaktır. Bu hususta çözüm aradaki güvenlik cihazının bu paketleri geçici hafızada depolayıp orijinal pakete imza denetimi uygulaması yönündedir.

- Parçalama başlığı ile en fazla 64K büyüklüğünde veri yollanabilmektedir. Ayrıca parçalama başlığı ile jumbo veri yükü başlığını birlikte kullanılamamaktadır (bkz. RFC–2460). Peki göndereceğimiz verinin büyüklüğü 64 K'dan büyük ve aradaki yolun MTU değeri de 64 K'dan büyükse ne olacaktır? Jumbo veri yükü özelliğini kullanamayız; çünkü, bu durumda tek paket halinde aktarım yapılamaz. MTU 64 K'dan büyükse parçalama işlemi de yapamayız çünkü bu değerde jumbo veri yükü seçeneğini kullanmamız gerekir ve iki başlığı aynı IP paketi içerisinde kullanamayız (bkz. RFC–2460).

  * Bahsedilen bu durumun oluşması kuvvetle muhtemeldir. Fakat böyle bir durum karşısında düğümlerin bu veriyi 64K büyüklüğünde parçalara ayırıp o şekilde hedefe ileteceğini düşünmekteyiz.

- Parçalanmış ilk paketin alınmasından itibaren 60sn'lik bir tampon bellekte tutma işlemi uygulanmaktadır [16]. Alıcı uçbirim 60 sn bekler ve bu süre sonunda aldığı paketleri birleştirir. Sonucunda işlem başarılı ise orijinal veri üst katmana iletilir; arada eksik bir paket varsa veya benzeri bir hata oluşmuşsa kaynak adrese ilgili ICMP hata mesajını gönderir. Bu yöntem birden çok uçbirim tarafından yapılan bir saldırıda suistimal edilebilir. Çok sayıda uçbirim aynı hedefe kasıtlı olarak eksik sayıda parçalanmış paket yollarsa alıcı durumundaki kurban uçbirim, her bir uçbirim için 60sn süre boyunca tampon bellek açacaktır. Bu alıcı uçbirimin belleğinin bir süre sonra dolmasına neden olacaktır. Bu sorun tabii ki IPv6'ya has bir sorun değildir. Bahsedilen parçalama işlemi IPv4'de de kullanılmaktadır. Dolayısıyla bahsettiğimiz bu problem, sözü edilen işlemin sahip olduğu potansiyel bir sorunu işaret etmektedir.

8.4. Alıcı/Hedef Ek-Başlığı

- Bu ek-başlık üzerinde herhangi bir öneri sunamadık. Çalışmalarımızın devamında üzerinde durmaktayız.

8.5. Doğrulama ve Emanet Verinin Paketlenmesi Ek-Başlıkları

Bu iki ek-başlığı IPSec protokolüne ait oldukları için tek başlık altında ele aldık. Başlık yapıları ve kullanılma amaçlarına yönelik herhangi bir güvenlik sorunu bulamamakla beraber IPSec ve buna bağlı olarak bu başlıklar hakkındaki güvenlik sorunu oluşturacağına inandığımız hususlar aşağıdaki gibidir:

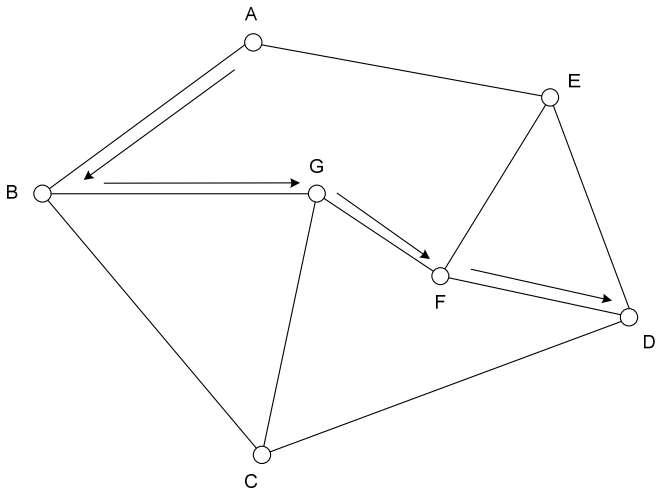
- Her iki başlık içerisinde ortak olarak bulunan ardışıklık numarası monoton artan bir sayıdır. Güvenlik birliği içerisinde aynı veri paketlerinin tekrar edilmemesi amacıyla kullanılan bu numara döngüye girmemektedir. Bu numaranın monoton artan bir sayı olması dolayısıyla, eğer emanet verinin paketlenmesi ek-başlığı kullanılmak suretiyle paket şifrelenerek iletilmiyorsa, ağ üzerinde paket gözleme yazılımı kullanan herhangi bir kişi ardışıklık numarası değerini öğrenip kendi kötü

amaçlı paketlerinde kullanmak için bir sonraki ardışıklık numarasını tahmin edebilir.

- IPSec protokolü uyarınca yineleme engeli işleminin bir parçası olan ve paketlerin doğru bir biçimde alınıp alınmadığının kontrolünün yapıldığı pencere yönteminde ise belirlenen bir pencere büyüklüğü kadar paket, bu pencere içerisinde incelenir. Bu yöntemde varsayılan pencere büyüklüğü 64'dür. Alınan paketlerde ardışıklık numarası en büyük olan paketin ardışıklık numarası N ise, N-W+1 ile N'de dahil olmak üzere bu aralıktaki paketler pencere içerisinde kalır ve bu paketlerin kontrol işlemi gerçekleştirilir. Pencere, ardışıklık numarası bu pencerenin sağ kenarında kalan paketten büyük olan başka bir paket geldikçe sağa kayar. Bu şekilde pencere ilerlemiş olur ve yeni paketler de incelenir. Yalnız bu noktada soruna yol açabilecek bir nokta bulunmaktadır. Zira gelen yeni bir paketin ardışıklık numarası pencerenin sağında kalacak şekilde ise pencere otomatik olarak kaydırılacaktır ve pencere içerisinde tüm paketlerin doğru bir şekilde ulaşıp ulaşmadığı kontrolü de yapılmayacaktır. Bu da doğru gelecek paketlerin yeni pencerenin solunda kalması ve otomatik olarak çöpe atılması demek olacaktır. Bütün bunların ışığında diyebiliriz ki; eğer kasıtlı bir şekilde ardışıklık numarası hedef düğümün pencere değerinden büyük olan paketler yollarsak, bu hedef düğümün bu iletişim esnasında kendisine gelen olağan diğer paketleri değerlendirebilmesini engeller, çünkü normal bir iletişim esnasında gelen paketlerin bir kısmının doğrulanmasını sürekli olarak engellemiş oluruz.

9. Ping-Pong Saldırısı ve Olası Çözüm Önerisi

Bu ek-başlıkta yönlendirme türü değerinin"0" olması durumunda bu başlık hedefe giden yolda geçilmesi gereken belirlenmiş düğümlerin adres bilgilerini içerisinde barındırır. Bu şekilde paketi alan her yönlendirici paketin gitmesinin istendiği bir sonraki hedefi paket içerisinden okur ve belirlenmiş bir sonraki hedefe paketi iletir. Böylece veri paketimiz hedefe belirlediğimiz özel bir yol üzerinden ulaşır.



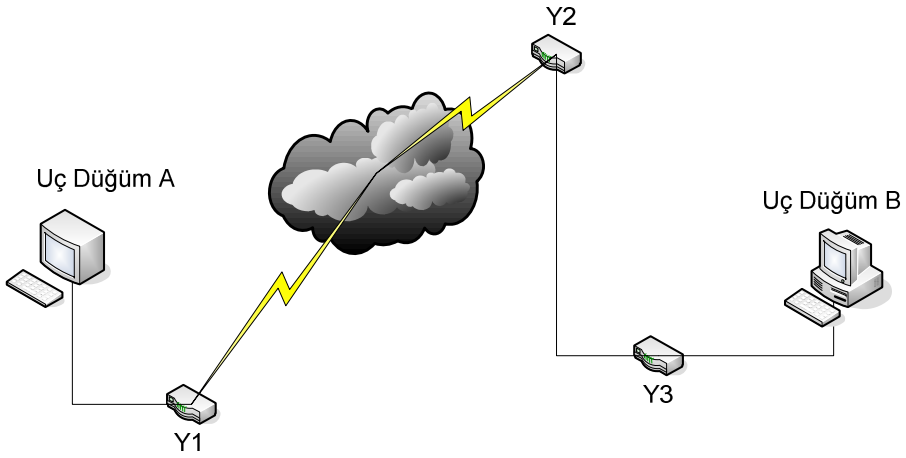
Şekil 13. Bir Ağda Yönlendirme Örneği

Yukarıda verilen şekilde A düğümünden D düğümüne gidecek bir paketimiz olsun. IPv4 protokolünün kullanıldığı durumda bu paketimiz herhangi bir yol üzerinden D düğümüne ulaşabilir. Günümüzdeki ağ yapısında paketin gideceği yol sadece yönlendiriciler tarafından belirlenebilir. Paketi alan yönlendirici kullandığı yönlendirme algoritmasındaki kriterlere göre paketi bir sonraki uygun hedefe aktaracaktır. Fakat buradan da anlaşıldığı üzere paketin kaynağı A düğümünün bu yolun belirlenmesinde söz hakkı yoktur. IPv6'da yukarıda bahsettiğimiz yönlendirme başlığı sayesinde kaynak A düğümü paketin iletiminde geçilecek ara düğümler hakkında söz sahibidir ve paketi kendi tercih ettiği bir yol üzerinden gönderebilme yeteneğine sahip olmuş olur. Bu şekle göre A düğümü paketi kendi tercih ettiği B-G-F rotası üzerinden D düğümüne iletebilecektir.

Yönlendirme başlığı içerisinde belirtilen ara düğüm adresleri *multicast* türü yayın adresleri olamazlar. Bu kısıtlama, protokolün tanımlandığı RC-2460 ve RFC-1883 numaralı standartlarda belirtilmiştir. Fakat yine aynı standartlar içerisinde kullanılacak ara düğüm adresleri ile ilgili başka bir kısıtlama getirilmemektedir. Şöyle ki, hedefimize ulaşırken paketin geçmesini istediğimiz ara düğüm adresi bir multicast adres değil fakat bir unicast veya anycast adres olabilir veya aslında var olmayan bir adres olabileceği gibi paketin o anda bulunduğu düğüme gelene kadar geçtiği düğümler içerisinde tekrarlanan düğümler

olabilir. Bu noktada özellikle üzerinde durduğumuz son fikri irdeleyecek olursak bu özelliğin nasıl yeni bir saldırı türünü ortaya çıkardığını daha iyi anlayabiliriz.

Standartta açıklanan yönlendirme başlığının çalışma ilkesi genel hatlarıyla şu şekilde olmaktadır:



Şekil 14. Yönlendirme Örneği Ağ Tasarımı

Uç düğüm A kaynağından B uç düğümüne giden bir paket için ara düğümlerdeki yönlendirme başlığı içeriği:

Kaynak Adresi	Uç Düğüm A
Hedef Adresi	Y1
Başlık Ek Uzunluğu	6
Kalan Segment	3
Adres[1]	Y2
Adres[2]	Y3
Adres[3]	Uç Düğüm B

Şekil 15.a. Örnek Yönlendirme: Y1 Yönlendiricisine İletilecek Paket

Kaynak Adresi	Uç düğüm A
Hedef Adresi	Y2
Başlık Ek Uzunluğu	6
Kalan Segment	2
Adres[1]	Y1
Adres[2]	Y3
Adres[3]	Uç Düğüm B

Şekil 15.b. Örnek Yönlendirme: Y1'den Y2 Yönlendiricisine İletilecek Paket

Kaynak Adresi	Uç düğüm A
Hedef Adresi	Y3
Başlık Ek Uzunluğu	6
Kalan Segment	1
Adres[1]	Y1
Adres[2]	Y2
Adres[3]	Uç Düğüm B

Şekil 15.c. Örnek Yönlendirme: Y2'den Y3 Yönlendiricisine İletilecek Paket

Kaynak Adresi	Uç Düğüm A
Hedef Adresi	Uç Düğüm B
Başlık Ek Uzunluğu	6
Kalan Segment	0
Adres[1]	Y1
Adres[2]	Y2
Adres[3]	Y3

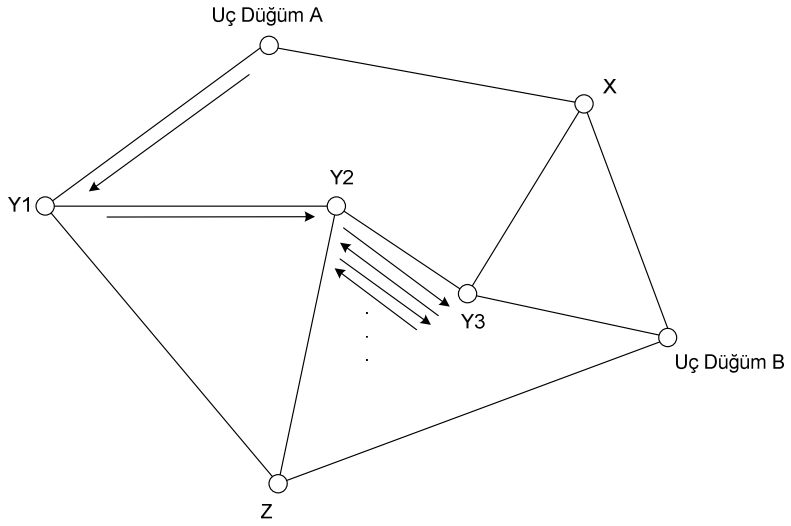
Şekil 15.d. Örnek Yönlendirme: Y3'den B Düğümüne İletilecek Paket

Standartlarca öngörülen işleyiş biçimi bu şekildedir. Fakat tekrar belirtmek gerekirse bu normal durumdaki işleyiştir. Aynı senaryoda ağ üzerine bırakılan paket şu şekilde olursa:

Kaynak Adresi	Uç düğüm A
Hedef Adresi	Y1
Başlık Ek Uzunluğu	14
Kalan Segment	7
Adres[1]	Y2
Adres[2]	Y3
Adres[3]	Y2
Adres[4]	Y3
Adres[5]	Y2
Adres[6]	Y3
Adres[7]	Y2

Şekil 16. Ping-Pong Saldırısı Yönlendirme Başlığı Parametreleri

Bu şekilde bir başlık kullanılması durumunda oluşacak trafik aşağıdaki şekildeki gibi olacaktır:



Şekil 17. Ağ Üzerinde Ping-Pong Saldırısı Sonucu

Tanımlanmış işleyiş mekanizması içerisinde düşünülecek olunursa böyle bir paketin doğurması beklenen sonuç, paketin Y2 ve Y3 düğümleri arasında 6 defa

iletilmesidir. Yukarıda öngörülen normal durumdaki senaryoda Y2 düğümü kendi üzerinden geçecek olan böyle bir paket için sadece 1 defa işlem yapmış olmaktadır. Fakat Ping-pong ismi koyduğumuz bu saldırı türü için uyarlanan son pakette ise tek bir paket, Y2 düğümünde 4 defa işlem görmüş olacaktır. Bu türde kullanılan paketler tekil kaynaklı saldırılarda ciddi sorunlara neden olmayabilir fakat servis engelleme saldırısının popülaritesinden bir şey kaybetmemesi ve gelecekte özellikle uç düğüm sayısındaki artış da göz önüne alındığında, bu tür bir saldırının fazla sayıda kaynaktan belirli birkaç ara düğüm üzerine gelmesi durumunda, bu ara düğümlerde ciddi sorunlara neden olabileceğini öngörmekteyiz.

Bu konuda yapmış olduğumuz tehdit öngörüsüne ek olarak bu tehdide karşı bir çözüm önerisi sunmaktayız. Şöyle ki, yönlendiriciler paketi aldıklarında ilgili yönlendirme başlığını gereken şekilde bir sonraki düğüme yönlendirmeden önce aşağıda belirtilen algoritma çerçevesinde incelemeli, kriterlere uygun bir paket olması durumunda paketi bir sonraki hedefe yönlendirmeli, aksi halde paketi çöpe atıp kaynak adresine gerekli şekilde tanımlanmış bir ICMP hata mesajı göndermelidir. Bu işlemi gerçekleştirecek algoritma şu şekildedir:

```
if( kalan segment <= (başlık ek uzunluğu/2)-2 )
{
     Bir önceki hedef= (başlık ek uzunluğu/2)-(kalan segment+1);
     İki önceki hedef= (başlık ek uzunluğu/2)-(kalan segment+2);

     if ( İki önceki hedef == Hedef adresi )
     {
           Paketi çöpe at ve kaynak adresine ilgili ICMP hata
           mesajını gönder
     }
     else if ( bir önceki hedef == Hedef adresi )
```

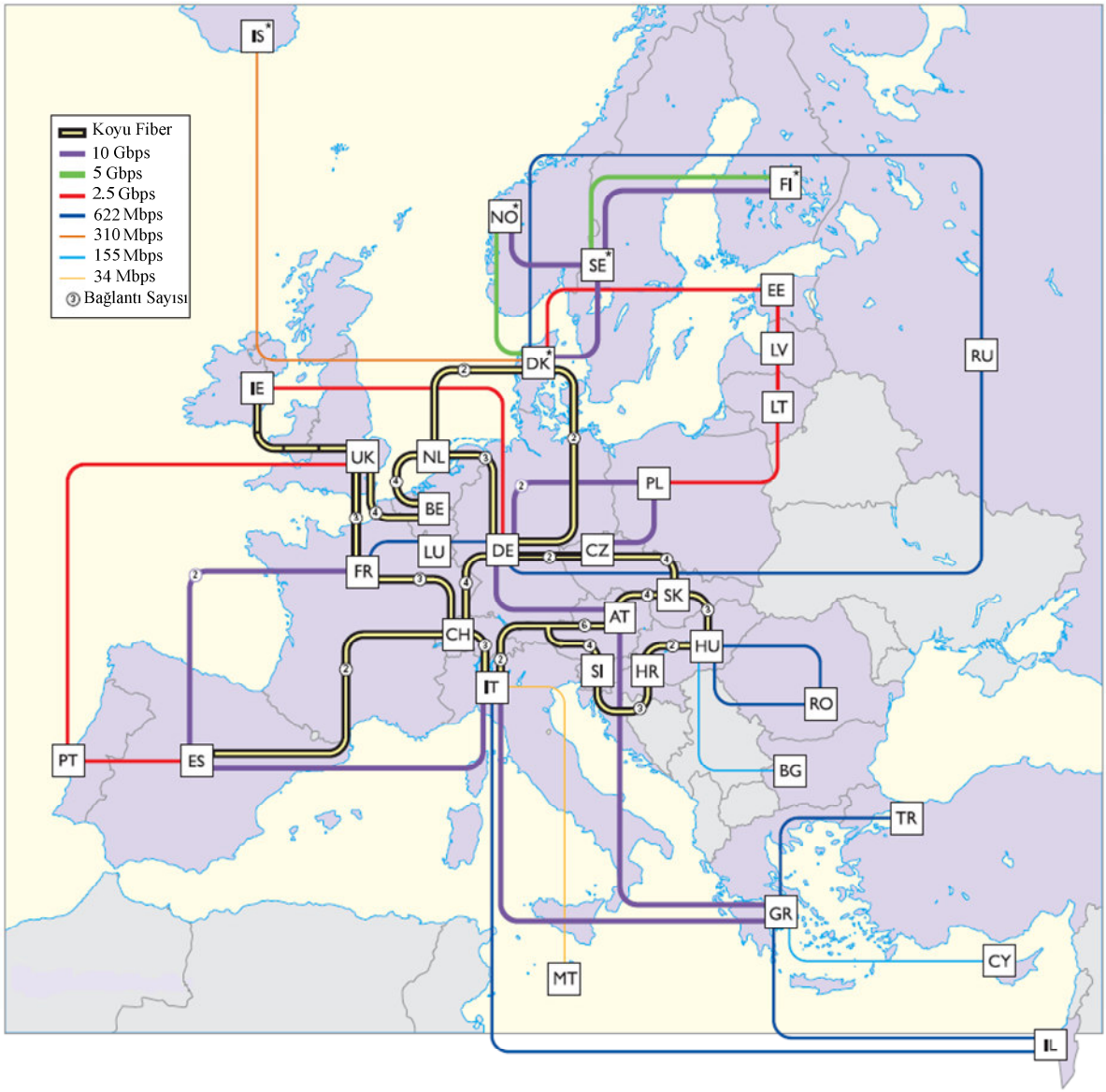
```
        {
                Paketi çöpe at ve kaynak adresine ilgili ICMP hata
                mesajını gönder
        }
}
```

RFC-2460'a göre yönlendirici paketi aldıktan sonra bu standartça tanımlanmış bir algoritma tarafından değerlendirilmektedir. Buna göre hata oluşturacak herhangi bir durum olmaması halinde algoritmaya göre bir indeks değeri olan *i* belirlenir. Bu, yönlendirme ek-başlığı içerisinde belirtilmiş ve paketin yol üzerinde ziyaret edeceği bir sonraki adresin tutulduğu alanın indeks değeridir. Bu değer ek-başlık içerisinde bildirilmiş ara adreslerin sayısından kalan segment değerinin çıkarılması sonucu elde edilir. Böylece yönlendirici ek-başlıkta 128 bitlik adres verilerinden oluşan diziler arasında, 0 indeks değerinden başlamak üzere, istediği adres bilgisine hemen ulaşabilir.

Önerdiğimiz bu algoritma öngördüğümüz Ping-Pong saldırısına önlem olarak sunulmuştur. Yönlendiriciler üzerinde uygulanması durumunda, az olmakla birlikte belirli bir gecikme oluşturması beklenmektedir. Bu algoritma, paketi değerlendiren düğüm ile öncesindeki 2 düğüm dahil olmak üzere toplam 3 düğüm arasındaki ve ara düğüm adreslerinin hep aynı düğümü işaret etmesi sonucunda aynı düğüm üzerindeki yerel çevrim atağı olarak niteleyebileceğimiz ataklara çözüm sunabilmektedir. Fakat arada toplam 4 veya üzeri ara düğüm olması durumunda bu çözüm etkisiz kalabilmektedir. Daha fazla sayıda ara düğüme yönelik benzer atakların önlenebilmesi için bu algoritmada değerlendirilen adres sayısı arttırılmalıdır, fakat bu da beraberinde yönlendiricinin daha uzun bir süre bu işlemle uğraşması ve de performansta belli düşüşün göze alınması gerekliliğini oluşturur.

EK-A

GÉANT2 Araştırma-Geliştirme Ağına Bağlı Ülkeler ve Omurgaya Erişim Hızları
(Ağustos 2005)



KAYNAKÇA

[1] JAMHOUR, E. ve STOROZ, S., "*Implementing Wireless Networks With Transition Mechanisms*", Proceedings of the XXII International Conference of the Chilean Computer Science Society (SCCC'02), IEEE 2002.

[2] WADDINGTON, D.G. ve CHANG, F., "*Realizing the Transition to IPv6*", **IEEE Communications Magazine.** June 2002, s.138-148.

[3] SAMAD, M., YUSUF, F., HASHIM, H. ve Md ZAN, Md MAHFUDZ., "*Deploying Internet Protocol Version 6 (IPv6) Over Internet Protocol Version 4 (IPv4)*", Student Conference on Research and Development Proceedings 2002, IEEE 2002.

[4] NAKAYAMA, T., NAKAMURA, Y. ve SUNAHARA, H. "A WWW Server Benchmark System in IPv6 Environment", Proceedings of the 2003 Symposium on Applications and the Internet Workshops (SAINT-w'03), IEEE 2003.

[5] COCQUET, P., "*IPv6 on DSL: The Best Way to Develop Always-On Services*", **PROCEEDINGS OF THE IEEE, VOL. 92, NO. 9,** SEPTEMBER 2004, s.1400-1407.

[6] ZEADALLY, S., WASSEEM, R. ve RAICU, I., "*Comparison of End-System IPv6 Protocol Stacks*", **IEE Proc.-Commun., Vol. 151, No. 3,** June 2004, s.238-242.

[7] LEE, HENRY C.J., MA, M., THING, VRIZLYN L.L. ve XU, YI., "*On The Issues of IP Traceback for IPv6 and Mobile IPv6*", Proceedings of the Eighth IEEE International Symposium on Computers and Communication (ISCC'03), IEEE 2003.

[8] METZ, C. ve TATIPAMULA, M., "*A Look at Native IPv6 Multicast*", **IEEE Internet Computing**, July-August 2004, s.48-53.

[9] LEE, Chu-Chuan., CHEN, Shao-Wei. ve CHANG, Pao-Chi., "*Active Packetization and Priority Description for Scalable Video over IPv6 Based Wireless Networks*", Proceedings of the 2004 International Symposium on Applications and the Internet Workshops (SAINTW'04), IEEE 2004.

[10] ZHAO, F., ve WU, S. F., "*Analysis and Improvement on IPSec Anti-Replay Window Protocol* ", Proceedings of IEEE International Conference on Computer Communications and Networks (ICCCN), October 2003, s.553-558.

[11] YAZAKI, T., KANETAKE, T., AKAHANE,S., SAKATA,Y., SUGAI,K., ve YANO, H., "*High-Speed IPv6 Router/Switch Architecture*", Proceedings of the 2004

International Symposium on Applications and the Internet Workshops (SAINTW'04), IEEE 2004.

[12] CHOWN, T. ve PALET, J., "*IPv6 R&D and Commerical Activities in Europa*", Proceedings of the 2004 International Symposium on Applications and the Internet Workshops (SAINTW'04), IEEE 2004.

[13] EFE, A. ve ÇÖLKESEN,R., "*Soket programlamada IPv4'den IPv6'ya geçiş ve yeni nesil uygulama önerileri*", **Akademik Bilişim 2005**, Gaziantep Üniversitesi, Gaziantep, 2-4 Şubat 2005.

[14] Microsoft Corporation., "**Introduction to IP Version 6**", September 2003(Updated March 2004).

[15] CONVERY, S. ve MILLER, D., "**IPv6 and IPv4 Threat Comparison and Best Practice Evaluation (v1.0)",** 11 March 2004.

[16] DEERING, S. ve HINDEN, R., "**Internet Protocol, Version 6 (IPv6) Specification**", RFC 2460, December 1998.

[17] HAENI,R.E., "**IPv6 vs. SSL, Comparing Apples with Oranges**", George Washington University, Washington DC., January 1997.

İnternet Kaynakları:

[18] The Apache Software Foundation, "Overview of new features in Apache 2.0", http://httpd.apache.org/docs/2.0/new_features_2_0.html, (Erişim: 22 Aralık 2005).

[19] Symantec Corporation, "**Symantec Internet Security Threat Report, Volume VII**", Published March 2005, http://ses.symantec.com/pdf/ThreatReportVII.pdf (Erişim: 9 Aralık 2005)

[20] GÉANT Project Homepage, "The GÉANT Network", http://www.geant.net/server/show/nav.128 (Erişim: 22 Aralık 2005).

[21] GÉANT2 Project Homepage, " The GÉANT2 Network", http://www.geant2.net/server/show/nav.740 (Erişim: 22 Aralık 2005).

[22] Information Society Technologies, 6NET Project Homepage, "About 6NET", http://www.6net.org/overview.html (Erişim: 22 Aralık 2005).

[23] Carnegie Mellon University, "CERT® Advisory CA-1998-01 Smurf IP Denial-of-Service Attacks", 13 March 2000, http://www.cert.org/advisories/CA-1998-01.html (Erişim: 9 Aralık 2005)

[24] University of California, The Cooperative Association for Internet Data Analysis(CAIDA), "The Spread of the Sapphire/Slammer Worm", www.caida.org/outreach/papers/2003/sapphire/sapphire.html (Erişim: 9 Aralık 2005)

[25] HINDEN,R.M., "**IP Next Generation Overview**", 1995, http://playground.sun.com/pub/ipng/html/INET-IPng-Paper.html (Erişim: 9 Aralık 2005)

[26] TÜBİTAK,ULAKBİM, "ULAKBİM Projeleri", http://www.ulakbim.gov.tr/hakkinda/projeler/ (Erişim: 22 Aralık 2005)