IPV6'da Güvenlik Açıklarına Genel Bir Bakış

Mehmet KARTAL*, Şeref SAĞIROĞLU, Halil İbrahim BÜLBÜL*****

*Gazi Üniversitesi, Institute of Informatics

**Gazi Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü

***Gazi Üniversitesi, Gazi Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Bölümü

ÖZET

Güvenlik ve adres ihtiyacı yanı sıra daha birçok yenilik içeren ve yeni bir protokol olan IPv6, sunduğu pek çok yeniliklerin yanı sıra bazı olumsuz yönleri de içerisinde barındırmaktadır. IPv4'ten kaynaklanan birçok güvenlik açığı ve adres ihtiyacı giderilmiş olsa da, geçiş sürecinin devam etmesi ve yeni protokolde tahmin edilemeyen veya kestirilemeyen açıklar sebebiyle de bazı olumsuz durumlar oluşabilecektir. Bu çalışmada yeni protokol ile ilgili yeniliklerden, güvenlik unsurlarından, yapısından, IPv4 ile benzerlik ve farklılıklarından bahsedilecek, bugüne kadar oluşan güvenlik açıkları sunulmuş, karşılaşılabilecek olumsuzluklara değinilmiş ve sonuçta genel olarak önerileri sunulmuştur.

Anahtar Kelimeler: IPv4, IPv6, Güvenlik, Güvenlik açıklıkları

An Overview to Security Vulnerabilities for IPV6 Networks

ABSTRACT

IPv6 has many advantages like security options and more address spaces but also has some disadvantages. Some of security vulnerabilities and lack of IP address as in IPv4 resolved in IPv6 networks. Moreover, IPv6 is not in use completely, transition to new protocol still goes on and unpredictable security vulnerabilities make new protocol disadvantageous. In this article, it will be mentioned new security options, similarities and differences between IPv4 and IPv6 networks, structure of new protocol, disadvantages of new protocol and some suggestions will be offered.

Keywords: IPv4, IPv6, Security, Vulnerability

1.GİRİŞ (INTRODUCTION)

Günümüzde sık olarak kullandığımız bilgiye ulaştığımız, iletişimimizi sağladığımız ve daha pek çok gündelik ya da kurumsal işlerimizi gördüğümüz sanal bir dünya haline gelen İnternet, dünya genelindeki milyonlarca bilgisayarın birbiriyle haberleşmesini sağlayan ağ bağlantısı olarak tanımlanmaktadır [1,2].

İş ve işleyişten haberleşmeye, uygulamalardan sosyal hayata pek çok alanımızı etkileyen internet, yeni bir yaşam yeni bir yaklaşım ve yeni bir çözüm olarak karşımıza çıkmaktadır.

Böyle büyük bir sistemin yönetimi ve kullanımı için iyi bir hiyerarşik yapı ve birçok kurallar dizisi gerekmektedir.

İnterneti oluşturan bu hiyerarşik yapının neredeyse en üst kısmında bulunan temel iletişim protokolüne İnternet Protokolü (IP) denmektedir. Bu temel protokolünün günümüzde de halen kullanılan sürümü IPv4, internetin yapısında uzun bir süre işlevini görmüş, başlıca sebep olarak internetin kullanımının katlanarak artması sonucu ihtiyaçları karşılayamaması sebebiyle yeni sürüm bir protokole ihtiyaç duyulmuştur. IPv4'ün sunmuş olduğu adresleme sayısı son blokların dağıtımıyla da son bulmuş olup, bu açığı kapatmak üzere geliştirilen yeni sürüm protokol IPv6'dır. Sunmuş olduğu imkanlar ile belirli bir geçiş süreci sonunda IPv4'ün yerini alacaktır.

Tablo 1'de IPv6 protokolünün IPv4 protokolüne göre üstünlükleri ve farklılıkları belirtilmiştir [3].

Tablo 1 IPv4 –IPv6 Arasındaki Farklılıklar [3]

Özellik Adı	IPv4	IPv6	Üstünlükleri
Adres Uzunluğu	32 bit	64 bit	Daha büyük adres uzayı
Başlıktaki sağlama (checksum) bilgisi	İçeriyor	İçermiyor	Hızlı yönlendirme
Başlıkta yer alan opsiyonlar	IP opsiyonları başlıkta yer alıyor	Kullanılacak IP opsiyonları, ek başlık ile ekleniyor	Hızlı yönlendirme
Parçalama (fragmentation)	Yönlendiriciler ve uçlar tarafından yapılıyor	Sadece uçlarda yapılıyor	Hızlı yönlendirme
Adresleme	Elle veya DHCP ile yapılabilir	Elle, otomatik veya DHCP ile yapılabilir	Kolay yapılandırma
IPSec desteği	IPSec desteği opsiyonel	IPSec desteği zorunlu	Kurulumda gelen IPSec desteği
Unicast, multicast, broadcast	Paketler unicast, multicast ve broadcast olarak gönderilebilir	Paketler unicast, multicast ve anycast olarak gönderilebilir	Az paket trafiği
Adres çözümleme	ARP protokolü kullanılır	Komşu keşfi (neighbour discovery) mesajları kullanılır	Az paket trafiği

* *Sorumlu Yazar (Corresponding Author)*
e-posta: bhalil@gazi.edu.tr
Digital Object Identifier (DOI) : 10.2339/2013.16.3, 119-127

Bu yeniliklere göre IPv6 birçok açıdan ihtiyacı karşılamakta ve performans açısından daha iyi olacağı beklenmektedir. Fakat 2008 yılında yapılan bir araştırmaya göre IPv6'ya geçiş hızının beklenilenden daha düşük olduğu gözlenmiştir [3]. Bunun sebebi geçiş maliyeti, IPv6 üzerinden verilen servislerin yeterli olmaması ve IPv4'ün halen kullanılabilmesidir. IPv6, IPv4 altyapısıyla uyumlu olduğu için, IPv6'ya geçiş sürecinin biraz daha devam edeceği düşünülmektedir. Aşağıda İnternet Mühendisliği Görev Gücünün tasarım aşamasında yeni protokol ile ilgili belirlediği hedefler [4,5] aşağıda listelenmiştir;

- Bütün sunuculara adres atayabilme,
- Performans açısından, yönlendirme tablolarının boyut bakımından IPv4 protokolüne göre iyileştirilmesi,
- Güvenliğin büyük ölçüde sağlanabilmesi,
- İnternet uygulamaları için, yeni protokolün daha iyi hizmet verebilmesi,
- Mobil cihazlarda sorunsuz bağlantının sağlanabilmesi,
- Yeni protokolün geliştirilebilir olması ve
- IPv4 protokolü ile uyumlu çalışabilmesi

Şu anki duruma bakıldığında bu hedeflerin birçoğunun gerçekleştiği gözlenmektedir. Fakat daha önce belirtildiği gibi yeni protokole geçiş sürecinin biraz daha zaman alacağı düşünülmektedir.

Bu çalışmada IPv6'nın tarihçesi, yapısı, IPv6'ya geçiş nedenleri, Türkiye'nin IPv6'ya geçiş sebepleri, IPv4 ve IPv6 arasındaki benzer güvenlik tehditleri, IPv6'ya geçiş sürecinde ortaya çıkan problemler ve IPv6'da güvenlik ve açıkları ele alınmıştır.

2. IPv6 (IPv6)

Bilgi çağında, internet üzerinden bilgiye daha güvenli daha hızlı erişebilmek, ses ve video gibi hızlı bir şekilde iletilmesi gereken verileri tanıyarak yüksek hızda iletim sağlamak, güvenlik desteğini üzerinde barındırmak, farklı cihazları tanımak ve tanımlamak, kolayca yapılandırmak, az paket ve ağ trafiği ile bu işlemleri yapabilmek artık istenilen ve kaçınılmaz hizmetler olmuştur [3,6].

Bu protokol yapısı ile ağlar, daha hiyerarşik bir yapıya kavuşmuş ve Ağ Adresi Dönüşümü (NAT) gibi işlemlere de artık gerek kalmamıştır [7].

2.1. IPv6'nın Tarihi (History of IPv6)

1990'lı yılların başında İnternet Mühendisliği Görev Gücü, adresleme ihtiyacını karşılamak için yeni protokolle ilgili çalışmalarını başlatmıştır [8].

IPv6 ile ilgili ilk çalışmalara 1990'lı yılların başında başlanmış, Temmuz 1992 yılında İnternet Mühendisliği Görev Gücü (IETF), IPv6 için öneride bulunmuş, 17 Kasım 1994'te yine IETF, Toronto toplantısında IPv6'nın taslağı oluşturulmuştur. İlk olarak Çin, 1998 yılında IPv6'ya geçiş çalışmalarını yapmış ve pratiğe dökmüştür. Daha sonra Japonya, Güney Kore ve Avrupa ülkeleri bu protokole geçiş çalışmalarını yapmışlardır. Amerikan Hükümeti, Haziran 2008 tarihinde yayınladığı bir bildiriyle 2025 yılına kadar bütün devlet ağlarının IPv6 olması ve yeni protokole geçişin tamamlanması gerektiğini belirtmiştir [9].

Türkiye'de geçiş çalışmaları 2001 yılında ULAKBİM tarafından başlatılmış, BTK'nın desteğiyle devam etmiştir. Daha sonra geçiş çalışmaları, 'Ulusal IPv6 Protokol Altyapısı Tasarımı ve Geçiş Projesi' adı altında ULAKBİM tarafından yürütülmüştür [9,10]. Bu projenin amacı, Türkiye'nin yeni protokole geçişi için yol haritası belirlemektir [11].

Bu çalışmalar 2003 yılından itibaren ULAKBİM ve TÜBİTAK tarafından yürütülmektedir. Bu zaman diliminde IPv6 ile FTP, DNS, SMTP gibi servisler erişilebilmektedir. TÜBİTAK ve ULAKBİM dışında BTK da (Bilgi Teknolojileri ve İletişim Kurumu) Türkiye'de IPv6 ile ilgili birtakım çalışmalarda bulunmuştur.

TÜBİTAK ve ULAKBİM tarafından yönetilen Ulusal Akademik Ağı (ULAKNET) 2003 yılından beri IPv6 bağlantısına sahiptir. Ayrıca ULAKNET ile üniversite ve araştırma kurumlarına IPv6 bağlantısı olanağı verilmektedir. ULAKBİM, üniversitelerin IPv6'ya geçişlerini sağlamak için ULAK6NET olarak anılan IPv6 Görev Gücünü kurmuştur [12].

2003 yılında ULAKBİM, IPv6 adres bloğunu alarak Avrupa Akademik ağı ile ilk IPv6 bağlantısını gerçekleştirmiştir. Daha sonra üniversiteler ve araştırma kurumlarının isteklerine göre IPv6 adresleri dağıtılmıştır.

Türkiye'de yeni protokolün kullanımını artırmak ve geçiş sürecinde oluşabilecek aksaklıklara karşı güvenlik testleri yapmak amacıyla Gazi ve Çanakkale 18 Mart Üniversiteleri ile TÜBİTAK, ULAKBİM bünyesinde IPv6-GO test laboratuvarları oluşturulmuştur [13,14].

Bu doğrultuda kurum ve kuruluşların IPv6'ya geçişleri için yeni protokole geçiş mekanizmaları üzerinde analiz yapılmakta ve en uygun olanı belirlemeye çalışılmaktadır. Oluşabilecek güvenlik sorunlarına karşı çözümler üretilmeye çalışılmış, geçiş için en uygun maliyet belirlenmiş ve bütün bu özellikleri yapabilecek bir karar destek sistemi geliştirilmiştir. Geliştirilen karar destek sistemine DESTAN adı verilmiştir ve bu sisteme http://ceng.gazi.edu.tr/destan adresinden erişilmektedir [15]. Bununla birlikte çeşitli konferanslar düzenlenmiş farkındalığı artırma adına eğitimler verilmiştir. Bu proje 2011 yılında tamamlanmış ve elde edilen sonuçlar, bilgiler ve belgeler "http://www.ipv6.net.tr" adresinde verilmiştir [15].

2.2. IPv6'nın Yapısı (Structure of IPv6)

Dünya üzerinde bir kullanıcıya bir IP adresi bile düşmemektedir. Bunun dışında internetin hızla gelişmesi, IPv4 adreslerinin dağıtımının iyi organize edilememesi yeni bir adresleme protokolünün gerekliliğini ortaya çıkarmıştır. Bu protokol IPv6'dır ve yeni protokol 128 bitlik yapısıyla ihtiyacın çok üzerinde adresleme olanağı sunmaktadır.

Bu sayede IPv6 kullanıcılara toplamda 2^{128} (340 282 366 920 938 463 374 607 431 768 211 456) adet

adres olanağı sunmaktadır. Onaltılık (hexadecimal) tabanda yazılır. Örnek bir IPv6 adresi şu şekildedir:

FDEC:0000:0000:0000:0000:0000:0000:0001 ya da FDEC::1

FDEC:0000:0001:0000:0002:0000:0000:0001

IPv6'da kısaltma yaparken sadece arada kalan her 16 bitlik kısımların hepsi 0 olduğunda ilk örnekteki gibi bir kısaltma yapılabilir.

Tablo 2 – IPv6 Başlık Yapısı

Sürüm (4-bit)	Trafik Sınıfı (8-bit)	Akış Etiketi (20-bit)
Yük Uzunluğu veya Boyutu (16-bit)	Sonraki Başlık (8-bit)	Atlama Sınırı (8-bit)
Kaynak Adresi (128-bit)		
Hedef Adresi (128-bit)		

IPv6'nın yapısına bakıldığında Tablo 2'de görüldüğü gibi ilk 4 bitlik alan adresin sürümünü göstermektedir. Yönlendiriciler bu kısımdan yararlanarak paket diğer kalan kısmını nasıl çevireceklerini belirler. IPv6 sürüm değeri 2'lik tabanda $(0110)_2$ yani onluk tabanda 6'ya denk gelmektedir. Trafik kısmı, 8 bitlik uzunluğa sahip olmakla beraber özel işlem gereken bir durumda veriyi işleme kolaylığı sağlamaktadır. Yani ses veya görüntü dosyasını diğer yapıdaki dosyalardan ayırt etmeye ve farklı şekilde iletim işlevini görmeye yaramaktadır. Akış etiketi, 20 bitlik uzunluğa sahip olup, ağ trafiğini kolaylaştırmaya yarayan kısımdır. Şöyle ki, aynı kaynak ve hedef IP adresinin olduğu iletimlerde, yönlendiriciler akışların izlerini sürerek aynı akışa ait paketleri daha verimli halde iletirler ve tekrar paket başlıklarını incelemek durumunda kalmazlar. IPv6'ya ait yük uzunluğu 16 bit olup, başlıktan sonra kalan kısmın yani taşınan verinin yükünü belirlemektedir. IPv6, ek başlıklarla daha büyük paket boyutlarını desteklediği için bu yük 64 KB sınırına kadar çıkmaktadır. Sonraki başlık kısmı protokol türünü içermektedir. Bu alana TCP, UDP ya da başla bir ek başlığın ismi yazılmaktadır. Atlama sınırı, IP paketinin ağda ne kadar ömrünün olduğunu belirten kısımdır. IPv6'da atlama sınırı sayısı, paketin ağda geçtiği her düğüm sonunda bir eksiltilir ve bu sayı 0 olduğunda paket yok edilmektedir. Böylece gideceği yeri bulamayan IP paketi yok edilmiş olur ve paketlerin sonsuz döngüye girmesi engellenmiş olunmaktadır.

RFC 2373 ve RFC 4291'de yeni protokolün 128 bitlik yapısı ve IPv6 paketlerinin kaynak noktası ile hedef noktalarını belirten özelliklerden bahsedilmiştir [16].

Bir paket iletimi yapılacağı zaman kaynak adres alanına göndericinin IP adresi hedef adres alanına da alıcının IP adresi yazılmaktadır. En küçük IPv6 adres değeri 0:0:0:0:0:0:0:0, en büyük adres değeri ise FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF'dir.

2.3. IPv6'daki Yenilikler (Improvements on IPv6)

IPv4, 2^{32} adet adresleme, IPv6 ise 2^{128} tane adresleme olanağı sunmaktadır. Bu durum yakın bir zamanda IPv4 adreslerinin tükeneceği göz önünde bulundurulursa IPv6'nın gereken miktarın çok üzerinde adres sayısı sunduğu görülmektedir.

Yeni protokol IPv6'nın önemli özelliklerinden biri de paket yapısındaki ek başlıklarıdır [17]. Ek başlıklar dinamik yapıda olup sadece ihtiyaç halinde kullanılmaktadır. IPv4'ün başlık yapısında ek başlık kullanılmasa bile datagramda bulunmaktadır. IPv6'da sadece ihtiyaç halinde ek başlıklar eklenir. Bunun sonucu gereksiz ek başlıkların IPv6 başlık yapısından çıkarılması ile hem zamandan hem de bant genişliğinden tasarruf edilmiş olur. IPv6'ya eklenen akış etiketi kısmı sayesinde, öncelikli iletilecek paketleri tanımlama olanağı sunulur. Bu hizmetlere örnek verilecek olursa; görüntülü konuşma, canlı video yayını, mobil hizmetler olabilir. IPv6'da adres yapılandırma işlemi otomatik olarak yapılabilmektedir. Bunun için iki yöntem bulunmaktadır. Birinci yöntemde, harici bir sunucu yardımıyla (DHCPv6), diğer yöntemle ise sunucusuz yapılandırma yapılabilmektedir. Ses, görüntü gibi gecikmesiz iletilmesi gereken, QoS (Quality of Service) uygulamalarında IPv6'nın başlığında bulunan 8 bitlik öncelik kısmı yeni protokolün önemli özelliklerinden biridir. Yeni protokolün başka bir özelliği, hareketli cihazlar için yüksek hızda bağlantı sağlayan altyapıya sahip olmasıdır [18].

Hareketli kullanıcılar, bulundukları noktadan bağımsız olarak kendi ev ağlarında tanımlı olmaktadırlar. Kullanıcı, kendi ev ağı dışında başka bir ağa bağlandığı durumda, kendisine sıla adresi atanarak ev ağına iletilen paketler ev ağından hareketli cihazına yönlendirilir.

2.4. IPv4'teki Temel Sorunlar (Basic Problems in IPv6)

IPv4'ün tasarım aşamasında, protokol uç uca (E2E) bağlantı modeli olduğu için içerisinde güvenlik protokolleri içermesi planlanmamış olsa da güvenliğin sadece uç noktalarda sağlanacağı tasarlanmıştır [19].

IPv6'ya geçilmesinin sebebi IPv4'te oluşan birtakım sorunlardan kaynaklanmaktadır. Bu sorunlar, IPv4'teki adreslerin tükenmesi, hiyerarşi desteğinin yeterli olmaması, karmaşık yapıdaki ağ yapılandırması ve IPv4'te oluşan güvenlik açıklarıdır [1,4,5].

IPv4, teorik olarak 2^{32} sayıda adresleme sunmuş olsa da verimsiz adres atamasından dolayı hiçbir zaman bu sayıya ulaşılamamıştır. Ne kadar iyileştirme çabaları yapılmış olsa da internet kullanımındaki hızlı artış artık IPv4'ün yetersiz kalmasına sebep olmuştur.

3. TÜRKİYE'NİN IPv6'YA GEÇİŞ SEBEPLERİ (TURKEY'S REASONS of TRANSITION to IPv6)

İnternetin, Türkiye'de kullanım oranının yüksek olduğu göz önünde bulundurulursa, IPv6'nın her yerde ve her cihazda kullanımının mümkün olması bu proto-

kole geçiş nedenlerinin başında gelmektedir. IPv6'da güvenliğin büyük oranda sağlanması nedeniyle bankacılık ve ticari alanda internet kullanımında artış sağlanacaktır.

Yeni protokolün uygulanmaya başlaması ile birlikte, güvenliğin birçok yönden sağlanmış olması sonucu, kurum ve kuruluşlar tarafından bu yönde yatırım projeleri yapılmaktadır [20].

IPv6 protokolü ile yüksek ve istikrarlı bağlantılar elde edilecektir. Ayrıca IPv6, hareketli cihazlarda uyumlu olma özelliği ile internet kullanımı artacaktır. Kablosuz ağların sayısında artış sağlanacak, ses, video, görüntü uygulamalarının IPv6 protokolü ile yüksek hızda desteklenmesi ile de bu yönde geliştirilen uygulamalarda artış gözlenecektir. Bu protokole geçiş sebeplerinden biri de e-devlet, tıp, savunma, ulaşım, tarım gibi alanlarda artacağı beklenirken, mobil sektörde de uygulamaların sayılarının artacağı IPv6'ya geçiş için önemli sebeplerdir.

4. IPv4 VE IPv6 ARASINDAKİ BENZER GÜVENLİK TEHDİTLERİ (SIMILAR SECURITY THREADS BETWEEN IPv6 AND IPv4)

IPv6'ya tamamen geçişin A.B.D. için 25 milyar dolara [21] ve ülkemiz için yaklaşık 1 milyon TL'ye [15] mal olacağı öngörülmektedir. Uzmanlara göre bu maliyetin bu kadar yüksek olmasının sebebi, yeni protokole geçiş aşamasında ağ elemanlarının yeni protokole uyum sağlaması sürecinde ağ güvenliğinde ciddi sıkıntılar oluşması ve oluşan güvenlik açıklarından saldırganların yararlanması ile ortaya çıkacak maddi kayıplar uzman personel eksikliği ve geçişte pek çok ağın, üzerinde kullanılan yazılımların değiştirilecek olmasıdır [7].

IPv4 için mevcut olan bütün saldırılar aynı zamanda IPv6 için de tehlike arz etmektedir. Bu tehditler, paket koklama saldırıları, ortadaki adam saldırıları, bellek taşırma saldırıları, uygulama seviyesi saldırıları, DHCP saldırıları ve sahte cihazlardır [19,22,23,24]. Bu saldırı türleri alt başlıklarda açıklanmıştır.

4.1. Paket Koklama Saldırısı (Package Sniffing Attacks)

Bu saldırı türü, ağdaki veri paketlerinin yetkisiz erişim sonucu elde edilip incelenmesidir [22]. Bu saldırı türü iki protokolde de etkili olabilmektedir. Fakat IPSec özelliğinin IPv6'da zorunlu olması dolayısıyla paket ele geçirilmiş olsa bile şifreli olacağından bu durum IPv6'da güvenli bir durum arz etmektedir. IPSec özelliğinin IPv6'da zorunlu olmasına rağmen kullanımı isteğe bağlı olduğundan dolayı bu durum güvenlik açığı oluşturabilmektedir. IPSec, kriptografik protokollerden oluşan ve ağ trafiğinde verinin şifrelenerek iletimini bununla birlikte veriye erişecek kullanıcının yetkilendirmesini sağlayan güvenlik protokolüdür [23].

4.2. Ortadaki Adam Saldırıları (Men in the Middle Attacks)

Bu tür saldırılarda, saldırganlar IP adresini taklit edebildiklerinden, saldırgan kurbana paket göndererek gerekli yetkileri kazandıktan sonra, kendisine gönderilen verileri yönetebilir ya da başka bir yere yönlendirebilmektedir [18].

Yeni protokolde IPSec kullanımı zorunlu olmasına rağmen, IPv4 ve IPv6 protokollerinin beraber kullanıldığı mekanizmalarda IPSec kullanımı zorunlu değildir ve bu saldırı türüne karşı savunmasız kalmaktadır [22].

4.3. Taşırma Saldırıları (Attacks of overflow)

Taşırma saldırıları ile saldırgan, hedefin kaldırabileceğinden çok fazla istek göndererek, karşı tarafın hizmet vermesini engelleyebilir. Bu saldırı, farklı cihazların aynı anda aynı hedefe istek göndermesi ile olur. Bu tür saldırılar hem eski hem de yeni protokolün adres yapısıyla bağdaşmadığından yeni protokolde herhangi bir değişiklik olmayacaktır [22].

IPv6'da adres uzayının büyümüş ve sahte IP'lerin tespitinin zorlaşmasından dolayı, bu tür saldırıları da tespit etmek zorlaşmıştır.

4.4. Uygulama Seviyesindeki Saldırılar (Attacks on Application level)

Bir sistemin güvenliği sadece basit bir elemana bağlı olmamakla beraber güvenlik birçok basamak ve katmandan oluşmaktadır. Örneğin sahte IP (IP spoofing), paket koklama (packet sniffing) gibi saldırılar uygulama seviyesi türü saldırılardır [24].

Bu tür saldırılara, uygulama seviyesinde uygulanan solucan dağılımı veya hafıza taşırma gibi saldırı türlerini de eklenebilir. Uygulama seviyesi türü saldırılar ağ topolojisi ile bağlantılı olmadığı için bu tür saldırılara IPv6'da engel olunamamaktadır. Sadece IPSec yetkilendirme ve şifreleme özelliği ile belli bir seviyede güvenlik sağlamaktadır.

Solucan dağılımı türü saldırılarda, solucanlar yayılmak için büyük miktardaki bant genişliğinden yararlanmakta ve ağdaki cihazlara kısa sürede bulaşmaktadır. Bu yüzden iletişim aksamakta servis kalitesi düşmektedir [19].

Genel olarak bakıldığında ise saldırıların veya güvenlik açıklarının en fazla bu seviyede olması beklenmektedir.

4.5. DHCP Saldırıları ve Sahte Cihazlar (Attacks of DHCP and Fake Devices)

IPv6'da DHCP sunucusu ortadan kaldırılmış fakat buna karşılık gelen yapıda yeni bir güvenlik mekanizması eklenmemiştir. Hedef cihaz için sahte olarak üretilen komşu istek paketleri, paketin komşu tanımlama önbelleğinin üzerine yazılarak IPv4'teki gibi güvenlik açığı oluşturmaktadır [18]. Sahte cihazlardan kasıt da ağ üzerinde yetkisi olmayan ve DHCP sunucusu, istemci, kablosuz erişim noktası gibi tanımlanabilen cihazlardır. IPv6'da bu değişmemiştir fakat IPSec özelliği

ile cihazların yetkilendirmesi ve bu tür sahte cihaz ataklarının engellenmesi mümkün olacaktır.

5. IPV6'DA OLUŞABİLECEK GÜVENLİK TEHDİTLERİ (PROBABLE SECURITY THREADS on IPv6)

Bu protokolde ve uygulamaların da meydana gelebilecek güvenlik açıkları, aşağıda alt başlıklar halinde verilmiştir.

5.1. Keşif Saldırıları (Attacaks of Reconnaissance)

Bu tür saldırılar normalde saldırı türü olmaktan çok, saldırının analiz aşaması olarak nitelendirilebilir. Çeşitli tarama yöntemleri kullanılarak ağdaki IP adresleri tespit edilir ve daha sonra port taraması gibi diğer işlemler uygulanır. IPv6'da alt ağ sayısı IPv4'e göre çok daha fazla olduğu için yeni protokol bu tür saldırılara karşı daha dayanıklı hale gelmektedir. Fakat IPv6'daki çok gönderim adresleri saldırgan tarafından ağdaki cihazları tespit etmek amacıyla kullanılabilir.

5.2. Ek Başlıklarla İlgili Tehditler

IPv6 ağlarındaki yönlendiricilerin gelen paketlerdeki yönlendirme başlıklarını işleyebilme özelliğinden dolayı yetkisiz erişim gibi güvenlik tehditlerine önlem alınamamaktadır [18].

Örneğin saldırgan, ağdaki bir cihaza yasaklı olan bir paketi gönderdiğinde, normal şartlarda yasaklı paketin süzülmesi gerekirken, cihaz paketi yönlendirmektedir. Böylece saldırgan sahte IP adresi kullanarak hedef cihaza hizmet dışı bırakma saldırısında bulunabilmektedir.

5.3. Geçiş Mekanizmaları (Transition Mechanisms)

IPv4 protokolünün halen kullanılmakta olması ve IPv6'ya geçişte uyum sorunlarının baş göstermesi sonucu bu sürecin beklenilenden daha uzun sürecektir. Uyum sorunlarını ortadan kaldırmak için birden fazla geçiş mekanizması oluşturulmuştur. Fakat oluşturulan mekanizmaların yanlış yapılandırılması sonucu tahmin edilemeyen güvenlik açıkları oluşabilecektir.

Yalın IPv4 ve IPv6 kullanan sunuculara göre ikili yığın kullanan sunucuların DOS (Denial of Service attacks) saldırılarından daha çok etkilendiği ve solucan yayılımına karşı ise yüksek risk taşıdığı rapor edilmiştir [25,26].

DOS (Denial of Service attacks) saldırıları, hedef sunucuya sürekli istek gönderilir ve sunucu isteklere cevap veremeyecek hale getirilerek hizmet vermesi engellenerek yapılır [23].

Tünelleme geçiş yönteminde, IPv6 desteği verildiği durumlarda trafiğin filtrelenmesi mümkün olmadığından, IPv4 adresi doğrulaması dışında kimlik doğrulaması yapılamamasının güvenlik açığı oluşturduğu belirtilmiştir [27].

Teredo geçiş yönteminde, RFC 4380'de meydana gelebilecek güvenlik açıkları; NAT yapısında delik açma, ortadaki adam saldırısı, servis kullanan ve kullanmayan uçlar olarak sıralanmaktadır. Aynı zamanda uygulamalarda güvenlik açıkları meydana gelebilmektedir [27,28].

Çevrimiçi yöntemlerde paket başlıklarında yapılan değişikliklerden dolayı, farklı protokoller ile kullanılma veya kullanılmama durumu güvenlik açıklarına sebebiyet verdiği, IPSec kullanarak şifreleme ve doğrulama uygulamalarında sıkıntılar çıktığı rapor edilmiştir [27].

5.4. Kötücül Yazılım Tehditleri (Malware Threats)

Kötücül yazılım, bilgisayar ağları için tehdit oluşturan, virüs, solucan, casus yazılım, truva atı olarak adlandırılan zararlı yazılımlara verilen genel bir addır [29]. Kötücül yazılımlar yayılmak en çok interneti kullanarak kullanıcılara zarar vermektedir.

Her gün dünya genelinde iki yüz elli milyon yeni kötücül yazılım üretildiği kaydedilmiştir [30].

Bu tür yazılımlar, salgın birer hastalık gibi bilgisayar ağlarında yayılmakta ve zararları ciddi maddi kayıplara yol açmaktadır. Her kötücül yazılımın farklı karakteristik saldırı yöntemleri vardır. Dosya paylaşımı, taşınabilir bellek paylaşımı bu yöntemlerden sadece birkaçıdır. Bununla birlikte kullanıcıların konu hakkında yeterli bilgiye sahip olmaması bu tür yazılımların amaçlarına ulaşmasını kolaylaştırmaktadır.

Kötücül yazılımlar yayılmak için ağ sistemlerini kullandığından, IPv6 ağlarında IPv4 ağlarından farklı olarak çok az bir yayılım hızı farkıyla yine aynı şekilde ağda yayılmaktadır ve yeni protokolde güvenlik sağlanamamıştır. Yayılım hızının daha yavaş olması yeni protokolde adres uzayının genişlemiş olması ve buna bağlı olarak 128 bitlik adres yapısından dolayı ağdaki düğümlerde adreslerin daha geç çözülmesidir.

5.5. Tünel Mekanizmaları Saldırıları (Attacks of Tunnel Mechanizms)

Yeni protokole geçiş mekanizmalarından biri olan tünelleme mekanizması ile IPv4 ve IPv6 protokolleri bir arada çalışabilmekte, bir protokol diğer protokolün içinde paketlenerek iletim sağlanmaktadır [22].

Tünelleme mekanizmasında IPv6'nın IPv4 içinde taşınmasında saldırgan kendini gizleme yöntemini kullanabilmektedir. Şu anda kullanılan güvenlik duvarları kapsüllenmiş ağ trafiğini filtreleyememektedir. Böylece saldırgan IPv4 üzerinden IPv6 paketlerine filtrelenmeden erişebilmekte, bu da güvenlik açığına sebebiyet vermektedir.

5.6. IPv6 Ağlarında Solucan Dağılımı (Worm Distribution on IPv6 Networks)

Solucanlar, ağda bir güvenlik açığı olması durumunda ağa sızarak sistem kaynaklarına erişim hakkı sağlamaya çalışan kötücül yazılımlardır [31]. Yayılım için ağdaki bant genişliğini kullanırlar ve güvenlik açığının derecesine bağlı olarak ağdaki cihazlara yayılırlar. Yayılımı gerçekleştirebilmek için sızdıkları sistemden sonra yeni konak arayarak diğer sistemlere de sızmaya çalışırlar. Solucanlar, internet solucanları, e-posta solu-

canları, P2P solucanları, anlık mesajlaşma solucanları olarak gruplandırılabilir [32].

Solucan dağılımı yeni protokol açısından bakılacak olursa, yayılım IP'ye bağlı olmamakla birlikte sadece yeni versiyonda konak arama metodları farklılık gösterecektir. Yeni protokole geçişte her iki versiyonunda kullanılacak olması, saldırı çeşitliliğini artıracağı için güvenlik sağlamak zorlaşacaktır. Bununla birlikte uygulama seviyesindeki ataklar, paket taşması [33] gibi IPv4 için geliştirilmiş saldırı türleri de yeni protokol için geçerliliğini koruyacaktır. IPv6 ağlarının yaygın olarak kullanılması ve güvenlik testlerinin sadece yerel ortamlarda yapılması protokolle ilgili bütün güvenlik açıklarının saptanmasına olanak vermemektedir. Yeni protokolün geliştirilme amaçlarından bir tanesi de hızlı yayılan solucanlara karşı önlem almaktır. Adres uzayındaki genişlik konak bulmak için IP taraması yapan solucanlar için dezavantaj olmaktadır. Fakat yeni protokoldeki bu özellik bunun için yeterli olmayacaktır.

Yeni protokolün özellikleri, solucanların işlevselliğini kolaylaştırabilir. Güvenlik yazılımlarının IPv4'e göre tasarlanmış olması ve yeni protokol için geliştirilecek güvenlik yazılımları yeni açıklar doğurabilecektir. Örneğin, OpenBSD işletim sisteminin [31] açıklarından bir tanesi, yeni protokol kaynaklıdır. Başka bir örnek verilecek olursa Windows işletim sisteminde IPv6'dan kaynaklanan servis dışı bırakma saldırısına imkan veren açıklar bulunmaktadır [31].

Yeni protokolün bilgisayar dışında mobil, PDA gibi cihazlarda da çalışacak olması ve geliştirilen güvenlik yazılımlarının çoğu bilgisayarlar üzerinde çalışıyor olması yeni güvenlik zaafiyetleri meydana getirecektir.

Solucan yayılımı başlangıç seviyesindeyken yakalamak ve gerekli tedbirleri almak bu bağlamda bir güvenlik tedbiri olabilir [34]. Bununla birlikte güvenlik ve diğer yazılımları güncellemek solucan dağılımına karşı alınabilecek diğer güvenlik tedbirlerinden biridir. Ayrıca solucan dağılımının tespiti için balküpü olarak adlandırılan saldırı tespit yazılımları kullanılabilir. Solucanlar yayılma aşamasında bulaştıkları adresler güvenlik duvarları tarafından kara listeye alınarak yayılım

Tablo 3 – IPv6'da Güvenlik Açığı Oluşturabilecek Casus Yazılımlar (Bu tablo [33] no'lu kaynaktan faydalınalarak genişletilmiştir)

Casus Yazılım Adı	**Köken**	**Hedef Platform**	**Yayılım Aracı**	**Tespit Yılı**	**Kullanılan Programlama Dili**	**Zarar(Milyon $)**
Flame	-	Tüm Donanım	Ağ	2012	-	-
Duqu	İsrail	Windos OS	MS Word	2011	-	-
Stuxnet	A.B.D. - İsrail	Windows OS	Siemens PLC	2010	-	-
Koobface	Rusya	Facebook	Mesaj Sistemi	2009	-	-
Brontok	Endonezya	Windows OS	E-posta	2006	-	-
Stration	-	Windows OS	E-posta	2006	-	-
Samy	Polonya	Myspace	XSS	2005	-	-
Bagle	Almanya	Windows OS	Mass Mailer	2004	-	-
Mydoom	Rusya	Windows OS	E-posta	2004	C++	38 500
Netsky	Almanya	Windows OS	E-posta	2004	C++	2 000
Caribe	İspanya	Symbian OS	Bluetooth	2004	C++	-
Santy	Güney Amerika	Web Sunucusu	PHPBB	2004	Perl	-
Blackworm	Asya	Windows OS	Mass Mailer	2004	Visual Basic	-
Sobig	-	Windows OS	E-posta	2003	C++	37 100
Sober	Almanya	Windows OS	Mass Mailer	2003	Visual Basic	-
Mylife	-	Windows OS	MS Outlook	2002	Visual Basic	-
Klez	Çin	Windows OS	E-posta	2001	C++	19 800
Sircam	Meksika	Windows OS	E-posta	2001	-	3 000
Iloveyou	Filipinler	Windows OS	MS Outlook	2000	Visual Basic	5 500
ExploreZip	İsrail	Windows OS	MS Outlook	1999	Delphi	1 020
Kak	-	Outlook Express	JavaScript	1999	Visual Basic	-
Happy99	-	Windows OS	E-posta & Usenet	1999	Assembly	-
Mytob	-	Windows OS	E-posta	-	-	-

engellenebilir. Tablo 3'te solucanların isimleri, kökenleri, hedef platformları, yayılım aracı, programlama dili ve verdiği ortalama zararlar yıllara göre listelenmiştir.

5.7. Yeni Güvenlik Açıkları (New Security Vulnerabilities)

Güvenlik açısından bakıldığında IPv4'te sonradan eklenen IPSec desteği, IPv6'da zorunlu olarak bulunmaktadır.

IPSec, IP paketlerinin kaynak noktasında şifrelenerek hedef noktaya varıncaya kadar güvenli ve sağlam bir şekilde iletimini sağlar [3].

Fakat IPv4 üzerinde IPSec özelliğinin kullanılması bazı sıkıntılara yol açmaktadır. Ağ Adresi Dönüşümü (Network Address Translation - NAT) IP paket modifikasyonunu güçleştirdiği için IPv6'da bu özelliği kullanmak daha kolaydır. IPv6'nın IPv4'ten ayrılan önemli özelliklerden biri de şifreleme ve kimlik denetimidir. Bunun için, uçtan uca ve ağ geçidinden ağ geçidine bağlantı olmak üzere iki farklı kip kullanılmaktadır. Bu kipler taşıma ve tünel kipleridir. Taşıma kipi, uçtan uca bağlantıda kullanılan kiptir ve bu kipte başlık hariç kalan kısımlar şifrelenir. Başlık kısmı genel olarak şifrelenmemesine rağmen kimlik denetimine dahil edilir. Şifrelemede AES-128 ve kimlik denetiminde SHA1 algoritmaları kullanılır. Tünel kipi ağ geçidinden ağ geçidine olan bağlantıda kullanılan bağlantı kipi olmakla beraber bu kipte IP paketinin tamamı şifrelenmektedir. Bununla birlikte yeni bir IP başlığı elde edilir. Şifreleme için AES-128 ve kimlik denetimi için SHA1 algoritmaları kullanılmaktadır. IPv4'te NAT kullanımıyla paketlerin parçalanması IPv6'da ortadan kaldırılmış olup, paket şifreli bir şekilde hedef noktaya kadar parçalanmadan iletilmektedir.

5.8. Kullanılan Casus Yazılımlar (Used Spyware)

IPv6 ağları tehdit edebilecek casus yazılımların listesi Tablo 3'te verilmiştir. Bu tablodanda görülebileceği gibi IPv4 ağları tehdit eden casus yazılımların çoğu IPv6 ağları da tehdit etmektedir. Bu yazılımlar daha çok C++ ile yazıldığı, menşeinin daha çok Almanya, İsrail, A.B.D. ve Rusya gibi ülkeler olsa da Meksika, Filipinler, Güney Amerika, Endonezya, Çin gibi ülkelerin de buna katkı verdiği, son dönemde ise geliştirilen yazılımların endüstriyel casusluk ve siber savaş amaçlı kullanıldıkları, daha çok Windows işletim sistemini kullandıkları ve Microsoft ürünleriyle yayıldıkları ve milyarlarca dolar zarar verdikleri tespit edilmiştir.

6. GENEL DEĞERLENDİRMELER (GENERAL EVALUATIONS)

IPv6'nın kullanılmasıyla ilgili olarak karşılaşılacak temel sorunlar; güvenlik, ağ ve sistem yöneticilerinin bilgi eksiklikleri, kullanılan yazılımların IPv6 desteğinin bulunmaması gibi hususlar olsa da güvenlik sistemlerinin de IPv6 desteği olmak zorundadır. Aksi halde güvenlik açığı oluşacak ve güvenlik yazılımları IPv6 ağlarına destek veremeyecek durumda olacaklardır. Örneğin güvenlik duvarı yazılımının IPv4 ve IPv6 ağlarının birlikte kullanıldığı yerlerde, IPv4 ve IPv6 ağlarındaki güvenlik kuralları birbirinden farklı olacağı için, ağ performansının daha iyi olması açısından IPv6'ya özgü ayrı bir güvenlik kuralları içeren güvenlik duvarı yazılımı kullanılması gerekir. Kurum içi görev yapan ağ ve sistem uzmanlarının bu konuda mutlaka eğitilmeli ya da bilgi sahibi olması gerekmektedir.

Burada karşılaşılabilecek ikinci problem ise IPv6 ağlarının yeni kurulması, üzerinde yeni yeni uygulamaların geliştirilmesi, yeni mimari yapıların kurulması ve protokol yapısında güvenlik zorunlu gelse de kolaylıkla yeni güvenlik açıklarının bulunması olasılığının yüksek olmasıdır. Bu konuda ağ kurulumu yapan ve yönetenlerin özellikle bu konuda bilgi sahibi olmaları ve uzmanlardan almaları gerekmektedir.

IPv6 ortamlarda meydana gelebilecek güvenlik açıklarına yönelik olarak henüz güvenlik çözümlerinin bulunmaması ve bundan dolayı da ilk geçenlerin ise sıkça güvenlik problemleriyle karşılaşmaları olasıdır. Ulusal IPv6 Projesi [11] kapsamında geliştirilen Balküpü [35] yazılımının bu tür açıkların bulunması ve ülkemizde bu alanda yapılacak çalışmaların önünü açması sebebiyle önemli bir çalışma olduğu ve karşılaşılabilecek problemlere çözüm sunması açısından önemli olduğu değerlendirilmektedir.

Sonuç olarak; karşılaşılabilecek problemlerin daha çok uygulamalarda ve farklı geçiş mekanizmalarının tercih edilmesinden dolayı güvenlik açıklarının meydana gelebileceği düşünülmektedir.

7. SONUÇLAR VE ÖNERİLER (RESULTS and SUGGESTIONS)

Çağımızın vazgeçilmez aracı internet, işlevselliği ve kullanıcı sayısının hızlı artışı ile daha güvenli hale gelmesi için üzerinde çok çalışılmaktadır. IPv6 protokolü yapılan çalışmalardan sadece biridir. Önceki sürüm protokole göre birçok açıdan iyileştirilmiş, önceki sürüm protokolde oluşan açıkların giderilmesiyle ilgili yenilikler yapılmış, fakat anlaşıldığı gibi bu durum yeterli olmamıştır. Güvenlik konusu çok geniş bir alan olduğu için internet güvenliğine sadece internet tarafından bakmamak gerekir. İnternetin işlevselliğini sağlayan protokoller ne kadar güvenli olursa olsun bu yeterli olmamaktadır. Kişisel veya kurumsal güvenliğin de sağlanması gerekir. Kişisel veya kurumsal bilgi ve verilerimizi korumak için, daha önce belirlenmiş güvenlik unsurlarını sağlamak gerekmektedir. Böylece hem kişi ve kurum tarafında hem de internet tarafında belirli bir yere kadar güvenlik sağlanmış olur. Güvenlikte her zaman güvenliğin yüzde yüz sağlanamayacağı gerçeğinden yola çıkılarak çalışmaları bu yaklaşım içerisinde yapmak en önemli adımdır.

Genel olarak dünyada IPv6 konusunda yapılan çalışmalar ve geçiş konusunda yapılan çalışmalar değerlendirildiğinde bu alanda yapılan çalışmaların yeterli olmadığı, IPv6'ya beklenen ilginin olmadığı, geçiş sürecinin ise beklenen düzeyde olmadığı

görülmüştür. Bu durumun pek çok sebebi vardır. Bu sebepler aşağıda maddeler halinde verilmiştir.

- IPv6'ya geçişin maliyetli olması ve yeni bilgi birikimi ve deneyim gerektirmesi,
- Eğitimli veya uzman personele duyulan ihtiyaç,
- Bilinmeyene ve yeni olan gelişmelere karşı tepki,
- Bu konuda teknoloji geliştiren ülkelerin sayısının sınırlı olması,
- IPv6'ya geçişte hizmet aksaması riskinin yüksek olması,
- Kullanılan yazılımların ve altyapının IPv6'ya geçiş maliyetlerinin yüksek olması,
- Uygulamaların ve altyapının birden değiştirilemeyecek kadar yaygın olması,
- İçerisinde pek çok fırsatları içerse de bu çalışmada da özetlendiği gibi içerisinde pek çok tehdit ve tehlikeyi barındırması,
- Tüm dünyada geçiş süreçlerinin uzun bir periyoda yayılması,
- Birimlerin, enstitülerin ve hatta ülkelerin geçiş maliyetini birden karşılayamamaları,
- Ülkelerin yeteri kadar internetten henüz faydalanmamaları,
- IP adres kıtlığının henüz yaygın bir problem olarak görülmemesi

Tüm bu olumsuzluklara rağmen IPv6 konusunda yapılan çalışmaların, geliştirilen uygulamaların, kullanılan teknolojilerin de artması, gelecekte IPv6 adresine duyulan ihtiyacın hızla artmasıyla da geçiş için hazır olunması ve gerekli tedbirlerin alınması önem arz etmektedir.

Ülkemizde bu yönde yapılan çalışmalara bakıldığında ülkenin stratejisinin olması, 2011'de yayımlanan Başbakanlık Genelgesiyle bunun taraflara bildirilmesi ve belirli tarihler verilmesinin bu konuda yaşanabilecek olan sıkıntıları azaltma açısından önemli olduğu kadar, IPv6 konusunda yapılabilecek yeni çalışmalarında önünü açacaktır.

Ülkemizde kurum ve kuruluşların IPv6'ya geçiş konusunda bilgi birikimlerini artırma, yapılan örnek çalışmaları inceleme, bu konuda yapılan çalışmaları öğrenme ve yapılan projeleri denemeleri açısından http://www.ipv6.net.tr [15] adresinde sunulan bilgilerin öğrenmelerinde, uygulamalarında ve özellikle belirtilen hususlara dikkat etmelerinde büyük fayda vardır.

8. TEŞEKKÜR (THANKS)

Yazarlar, TÜBİTAK-KAMAG birimine 108G100 no'lu "Ulusal IPv6 Protokol Altyapısı ve Geçişi Projesi"ne maddi katkılarından dolayı teşekkür ederler.

9. KAYNAKLAR (REFERENCES)

1. SAĞIROĞLU, Ş., AKTAŞ, M., "IPv6: Uluslararası Çalışmalar ve Türkiye'de Durum", ***IPV6 Konferansı***, Ankara, 5-10, 12 Ocak 2011.
2. BÜLBÜL, H.İ., TANYERİ, U., ŞAHİN, Y.G., "İnternet Protokolü v6 ve Geçiş Süreci", ***The Proceeding of 8th International Educational Technology Conference***, Eskişehir, Mayıs 2008.
3. YÜCE, E., "IPv4, IPv6 ve IPv6 Geçiş Yöntemleri Performans Karşılaştırılmaları***", IPv6 Konferansı***, Ankara, 27-30, 12 Ocak 2011.
4. LOSHIN, P., "IPv6: Theory, Protocol and Practice", 19-25, San Francisco, USA, 2003.
5. BRADNER, S., MANKIN, A., "The Recommendation For The IP Next Generation Protocol", ***IETF, RFC 1752***, USA.
6. BOLAT, A., CANBAY, C., CENGİZ, H., ÇETİN, T., KAR, M., KÜÇÜKÜNSAL, J., "Ulusal IPv6'ya Geçiş ve Stratejiler", ***4. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı***, 6-8 Mayıs 2010.
7. ROWE, B., GALLAHER, M., "Could IPv6 Improve Network Security? And, If So, at What Cost?", ***A Journal Of Law And Polıc***, 2 (2): 231- 267 (2006).
8. SOYLU, M.Y., AYDOĞAN, E., ÇETİN, S., GENCER, C., SAĞIROĞLU, Ş., "IPv4'ten IPv6'ya Geçiş İçin Örnek Bir Karar Destek Sistemi Modeli: GEMKAR", ***IPv6 Konferansı***, Ankara, 37-42, 13 Ocak 2011.
9. BEKTAŞ, O., SOYSAL, M., ORCAN, S., "Türkiye için IPv6 Geçişi Zaman/Aşama Planı Önerisi", ***Ulusal IPv6 Konferansı***, Ankara, 11-18, 12 Ocak 2011.
10. ALKAN,M., KARACAN, H., ORCAN, S., SAĞIROĞLU, Ş., ÜNVER, M., YAVANOĞLU, U., "Ulusal IPv6 Protokol Altyapısı Tasarımı Ve Geçişi Projesi: Anket Çalışması", ***Ulusal IPv6 Konferansı***, Ankara, 19-26, 12 Ocak 2011.
11. YÜCE, E., BEKTAŞ, O., ORÇAN, S., GÖKIRMAK, Y., SOYSAL, M., ÜNVER, M., ALKAN, M., SAĞIROĞLU, Ş., YÜCEL, N., "Ulusal IPv6 Protokol Altyapısı Tasarımı ve Geçişi Projesi", ***EMO Elektrik-Elektronik, Bilgisayar ve Biyomedikal Mühendisliği Ulusal Kongresi***, ODTÜ Ankara, 24 Aralık 2009.
12. BEKTAŞ, O., SOYSAL, M., ORCAN, S., "Türkiye İçin IPv6 Geçişi Zaman/Aşama Planı Önerisi", ***IPv6 Konferansı***, Ankara, 11-18, 2011.
13. BEKTAŞ, O., YÜCE, E., KOÇ, N., GÜRCAN, İ., ORCAN, S., "IPv6-GO Test Ağı Kurulumu", ***3. Haberleşme Teknolojileri ve Uygulamaları Sempozyumu***, İstanbul, (2009).
14. YÜCE, E., GÖKIRMAK, Y., "IPv6 Saldırı Araçları ve IPv6-GO Uygulamaları", ***4. Uluslar arası Bilgi Güvenliği ve Kriptoloji Konferansı***, ODTÜ Ankara, 1-7, 2010.
15. Ulusal IPv6 Protokol Altyapısı ve Geçişi Projesi, Bağlantı: http://www.ipv6.net.tr/, 27.07.2012.
16. AKŞİT, İ., "IPv6 Yapılandırılması ve Soket Tabanlı IPv6 Destekli Sunucu Yazılımı Geliştirme", Yüksek Lisans Tezi, ***Gazi Üniversitesi Bilişim Enstitüsü***, Ankara, 10-90, (2011).
17. BEKTAŞ, O., SOYSAL, M., "Yeni Nesil IP (IPv6) ve Güvenlik", ***InetTR 2006***, Ankara, 2006.
18. AYDIN, M.A., ÇAKIN, A., "IPv4/IPv6 Güvenlik Tehditleri ve Karşılaştırılması", ***4. Ağ ve Bilgi Güvenliği Sempozyumu***, Ankara, 25-26 Kasım 2011.

19. SOTILLO, S., "IPv6 Security Issues", ***The Information Security Writers***, The Infosec Writers Text Library, (2006).
20. BOLAT, A., TÖZER, A., "IPv6 ve Türkiye", ***Akademik Bilişim'09 - XI. Akademik Bilişim Konferansı Bildirileri***, 11 – 13 Şubat 2009.
21. POWNER, D.,A., RHODES, K., A., "Internet Protocol Version 6: Federal Government in Early Stages of Transition and Key Challenges Remain", ***United States Government Accountability Office 06 - 675***, ***Washington***, 1 – 13, 30 Haziran 2006.
22. BEKTAŞ,O., SAĞIROĞLU, Ş., SOYSAL, M., "Güvenlik Penceresinden IPv4/IPv6 Karşılaştırılması". ***3. Uluslararası Katılımlı Bilgi Güvenliği Ve Kriptoloji Konferansı***, Ankara, 132-138, 25-27 Aralık 2008.
23. GADONG, J., "IPv6-to-IPv4 Transition And Security Issues", ***Information Technology Protective Security Service***, Information Technology & State Store Building, 3-5, 2008.
24. Lioy, A., "Security Features of IPv6", Network Security,152-165, 1997.
25. TING, L., XIAOHONG, G., QINGHUA, Z., "A New Worm Exploiting IPv6 and IPv4-IPv6 Dual-Stack Networks: Experiment, Modeling, Simulation, and Defense ", ***IEEE Network***, 23(5): 22-29 (2009).
26. ÇALIŞKAN, B., BEKTAŞ, O., "IPv6 İkili Yığın Geçiş Yönteminde Uygulamaların Saldırı Altında Performans Analizi", ***3. Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı***, Ankara, 146-151, (2008).
27. YÜCE, E., GÖKIRMAK, Y., BEKTAŞ, O., ORCAN, S., "IPv6 Geçiş Yöntemleri Güvenlik Analizi", ***3. Haberleşme Teknolojileri ve Uygulamaları Sempozyumu***, İstanbul, Aralık 2009.
28. HUITEMA, C., "RFC 4380", ***IETF 4380***, ***RFC Report***, 38-45, 2006.
39. CANBEK, G., SAĞIROĞLU, Ş., "Bilgi ve Bilgisayar Güvenliği: Casus Yazılımlar ve Korunma Yöntemleri", ***Grafiker***, Ankara, 2006.
30. ZULKIFLEE , M., FAIZAL, M.A., MOHD FAİRUZ I.O., NUR AZMAN A., SHAHRİN S., "Behavioral Analysis on IPv4 Malware in both IPv4 and IPv6 Network Environment", ***International Journal of Computer Science and Information Securit***, 9(2): 10-15 (2011).
31. Bektaş, O., SOYSAL, M., "IPv6 Ağlarında Solucan Dağılımı", ***2. Haberleşme Teknolojileri ve Uygulamaları Sempozyumu***, İstanbul, (2008).
32. TANG, Y., LUO, J., XIAO, B., WEI, G., "Concept, Characteristics and Defending Mechanism of Worms", IEICE Transactions of Information and Systems, E92-D: (5), 799-809, 2009.
33. YAVANOĞLU, U., ÖZDEMİR, S., SAĞIROĞLU, Ş., "IPv6 Ağlarda Solucan Dağılım Saldırıları ve Önlemler", ***5. Uluslar arası Bilgi Güvenliği ve Kriptoloji Konferansı***, Ankara, 3-10, 17-18 Mayıs 2012.
34. CLIFF, C., ZOU, W.G., TOWSLEY, D., "The Monitoring And Early Detection Of Internet Worms", ***IEEE/ACM Transactions On Networking***, 13: (5), 961-974, Ekim 2005.
35. GÖKIRMAK, Y., BEKTAŞ, O., SOYSAL, M., YİĞİT, S., "Sanal IPv6 Balküpü Ağı Altyapısı: KOVAN", IPv6 Konferansı, ANKARA, 49-56, 13 Ocak 2011.