Çoklu Protokol Etiket Anahtarlamalı Ağlarda (MPLS) Güvenlik

İzzet Fatih Şentürk[1] Abdulsamet Haşıloğlu[2]

[1,2]Bilgisayar Mühendisliği Bölümü, Atatürk Üniversitesi, Erzurum
[1]e-posta: izzetfatih@atauni.edu.tr [2] e-posta: asamet@atauni.edu.tr

Abstract

The migration of Multi Protocol Label Switching based solutions is on the rise in the market today. *MPLS* provides enhanced scalability and high availability. But concerns still exist about the security features of *MPLS*. By nature *MPLS* does not provide encryption and can not protect the data confidentiality. Some approaches are suggested to increase the security of *MPLS*. This paper analyzes some of these approaches: *MPLS-VPN* and *MPLS-VPN-IPSec*. Security threats are compared and security properties which these approaches meet are analyzed. It also discusses strategies that can be implemented to provide an optimum security for networks.
Keywords: *MPLS, VPN, IPSec, Security*

1. Giriş

Bilgisayar ağları üzerinden her geçen yıl daha fazla bilgi geçiyor. Özel şirketler, kamu kuruluşları biz bireysel kullanıcılar bu bilgi ağlarına daha fazla bağımlı hale geliyoruz. Bu ağlarda dolaşan bilgiler sadece nicelik olarak artmıyor. Verimlilik artışı sağlayan kompleks yazılımların geliştirilmesi, stratejik öneme sahip sistemlerin bu bilgi ağlarına bağlanmasına ve ağlar üzerinde kritik bilgilerin dolaşmasına neden oluyor. Bilgisayar ağlarında stratejik öneme sahip bilgilerin daha fazla dolaşması bu ağlara yapılacak saldırıları daha cazip hale getiriyor. Makalemizde bilgisayar ağlarında güvenlik konusunu her geçen gün kullanımı artan *MPLS* teknolojisi perspektifinden inceliyoruz. *MPLS*'in *VPN* (*Virtual Private Network*) ile etkili kullanımı, sağladığı hizmet kalitesi (*QoS*), trafik mühendisliği (*TE*) ve yüksek erişilebilirlik ile ölçeklenebilir ve esnek olması gibi nedenlerden dolayı kullanımı hızla artmaktadır [1]. Güvenlik, MPLS'in temel geliştirme nedeni değildir [2]. Artan MPLS kullanımıyla birlikte güvenliğin daha fazla talep edilmesi, MPLS'in güvenliğin artırılması için araştırmacılar ve servis sağlayıcılar tarafından yeni yaklaşımlar ortaya konmasına neden olmaktadır [3]. *MPLS* mimarisinde güvenliğin artırılması için ortaya atılan yaklaşımlardan birisi *VPN* ile birlikte kullanılma durumudur [4, 5]. *ATM (Asynchronous Transfer Mode)* veya *Frame Relay* üzerinde kullanılan *VPN*'in *MPLS* ile kullanılması durumunda da aynı güvenlik özelliklerini gösterebileceği söylenmektedir [6]. Ancak yeni çalışmalarda bu durumda da güvenlik zafiyetleri bulunabileceği iddia edilmiştir [7]. *MPLS* sinyal güvenliği ve *RSVP-TE* sinyal güvenliği analizleri ile *MPLS* ağlarda kontrol mekanizmasının güvenliğinin sağlanması için bazı yaklaşımlar ortaya konmuştur [8, 9]. Ayrıca çoklu rota kullanımı ile güvenliğin arttırılması için yeni yöntemler ileri sürülmüştür [10].

Makalemizde *MPLS*'in şu anda yaygın olarak kullanılan *VPN* ile beraber kullanılma durumu ele alınacak ve güvenlik analizi yapılacaktır. Ardından bu mimariye *IPSec* (*Internet Protocol Security*) eklenmesi durumundaki güvenlik analizi uygulanacaktır. Alt katmanlar da dâhil olası güvenlik sorunları anlatılarak yüksek güvenlikli bir *MPLS* ağının oluşturulması hedeflenmektedir. Makalenin ilk kısmında güvenlik ve güvenlik özellikleri bilgisayar ağları kapsamında incelenerek hangi güvenlik özelliğine ne zaman ihtiyaç duyulacağı üzerinde durulacaktır. Sonraki kısımda *MPLS* hakkında bilgi verilerek *VPN* ve *IPSec* ile beraber kullanılma durumları ve bu alternatiflerin güvenlik riskleri üzerinde durulacaktır. Son kısımda ise ileride yapılabilecek çalışmalar hakkında bazı fikirler sunulmuştur.

2. Güvenlik ve Güvenlik Özellikleri

Şirketlerin verimliliği artırmak için bilgisayar sistemlerini kurumsal kaynak planlama sistemleriyle dışarıya açması, savunma sistemlerinin ve enerji nakil hatlarının bilgisayarlı destek sistemlerine bağlanması, internetin yaygınlaşması ve kişisel bilgilerin kolay erişilir hale gelmesi gibi nedenler bilgisayar sistemlerine ve bilgisayar ağlarına olan güvenlik kaygılarını artırmaktadır. Güvenlik kaygılarının giderilebilmesi için güvenlik beklentilerinin doğru belirlenerek buna uygun çözümlerin sunulması gerekmektedir. Farklı işlevlere sahip sistemler farklı güvenlik beklentilerine sahip olabilir. Güvenlik beklentileri genellikle bu üç güvenlik özelliğiyle ifade edilir [11].

a. *Mahremiyet (Confidentiality):* Hangi bilgiye kimlerin erişebileceğini ifade etmek için kullanılır. Mahremiyet özelliğinin sağlanmadığı bir ağda iki bilgisayar arasındaki veri alışverişi sırasında üçüncü bir bilgisayar bu verilere ulaşarak bu verileri anlamlı bir bilgiye dönüştürebilir. İletilen bilginin içeriğinin korunmasının dışında bilginin kimler arasında, ne zaman ve hangi yoğunlukta iletildiği de mahremiyet özelliğiyle korunması gerekir. Bunların korunmaması diğer güvenlik özelliklerine zarar verebileceği gibi doğrudan veya dolaylı olarak da mahremiyet özelliğine zarar verebilir. Yasadışı bir internet sitesinin sunucusuyla düzenli veri alışverişinde bulunan bir bilgisayarın tespit edilmesi, bir ağa bağlı sunucuların veri alışveriş yoğunluklarına bakılarak ana sunucunun tespiti, vergi borçlularının işlemlerinin yönetildiği bir sunucuyla hangi bilgisayarların iletişim kurduğunun takibinin yapılabilmesi mahremiyet özelliğinin sağlanmadığı ağlarda mümkündür.
b. *Bütünlük (Integrity):* Hangi değişikliklere izin verilebileceğini belirtmek için kullanılır. İki bilgisayar arasında devam eden veri iletimi sırasında üçüncü bir bilgisayarın bu verileri topladığını ama mahremiyet özelliği sağlandığı için anlamlı bir bilgiye dönüştüremediğini düşünün. Bu bilgisayarın

her ne kadar verileri anlamlandıramasa da içeriklerini değiştirerek iletişime müdahale etmesi ve bahsi geçen 2 bilgisayar aldıkları verilerin içeriklerine müdahale edildiğini anlayamaması ağın bütünlük özelliğini garanti edemediği gösterir. Uygun girdiler için uygun çıktıların oluşturulması da bütünlük özelliği ile korunur. Bir *yönlendirici* (*router*) ara yüzüne işleyebileceğinden fazla veri gelmesi ve sadece bir kısım verinin işlenebilerek, işlenemeyen verilerin *yönlendirici* tarafından göz ardı edilmesi o sistem için bütünlük özelliğinin sağlanmadığı anlamına gelir.

c. *Uygunluk (Availability):* Bilgi giriş çıkışının ne zaman yapılabileceğini belirtmek için kullanılır. Uygunluk özelliğini iyi şeylerin çalışma zamanında olması şeklinde ifade edebiliriz. İletişimin kesilmeden devam edebilmesi veya bir *yönlendiriciye* gelen paketlerin adil bir şekilde hedeflerine yönlendirilmeleri uygunluk özelliğinin sağlandığını gösterir. İki bilgisayar arasında devam eden iletişimin hizmetin engellenmesi (*DoS*) saldırısıyla kesilmesi ağ için uygunluk özelliğinin garanti edilemediğini gösterir.

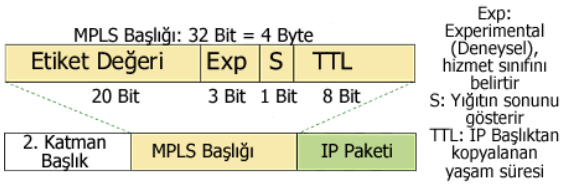
Kısaca özetleyecek olursak iki bilgisayar arasında devam eden iletişim için uygunluk özelliğinin garanti altına alınması *sistem çalışıyor*, *A* bilgisayarından gönderilen bilgi *B* bilgisayarına ulaştı anlamına gelir. Buna Bütünlük özelliğinin de eklenmesi *sistem düzgün çalışıyor*, *A* bilgisayarından gönderilen bilgi içeriği değiştirilmeden *B* bilgisayarına ulaştı anlamına gelir. Mahremiyet özelliğinin de eklenmesi *sistem düzgün ve güvenli bir şekilde çalışıyor A* bilgisayarından gönderilen bilgi sadece *B* bilgisayarının anlayabileceği şekilde ve bozulmadan *B* bilgisayarında ulaştı anlamına gelir.

Bu güvenlik özelliklerinin kullanılan sistem için belirlenmesi güvenliğin sağlanması açısından önemlidir. Mesela tamamen güvenilir sistemlerden oluşan ağda performans tercih edilip mahremiyet gerekli görülmeyebilir. Bu yüzden bir Servis Sağlayıcı, Kurum veya son kullanıcı için sistemlerin büyüklüğünün işlevlerinin ve kullanıcılarının farklılığı güvenlik ihtiyaçlarının da farklı olmasına sebebiyet vermektedir. Bir servis sağlayıcı için gerekli olan bir güvenlik özelliği bir kurum için gerekli olmayabilir veya Mimarileri farklı olduğu için iki kurum farklı güvenlik özelliklerine ihtiyaç duyabilir. Her güvenlik özelliği her zaman gerekli olmayabileceği gibi bazı durumlarda güvenlik tamamen ihtiyaç dışında kalarak performans ve hız daha önemli durumda olabilir. Güvenlik ihtiyaçlarının neler olduğunun belirlenmesi güvenli bir sistem için gereklidir.

3. Çoklu Protokol Etiket Anahtarlama (MPLS)

MPLS, çoklu protokol etiket anahtarlama olarak ifade edilen, OSI katmanındaki *ikinci* ve *üçüncü* katmanlar arasında çalışan bir ağ protokolüdür. *IP (Internet Protocol), ATM* ve *Frame Relay* gibi ağ protokolleri ile birlikte çalışabilmesi çoklu protokol şeklinde tanımlanmasını sağlar. *MPLS* başlığı içinde etiketler bulunur (bkz. *Şekil 1*). Bu etiketler sayesinde etiket temelli anahtarlama yapılması, paketlerin üçüncü katmanda yönlendirilmesine gerek kalmadan ikinci katmanda anahtarlama yapılabilmesini sağlar. MPLS kullanılan ağda kaynaktan hedefe verinin takip edeceği rotanın *ATM, Frame Relay* veya *Ethernet* gibi birden fazla ikinci katman teknoloji üzerinden geçebilmesi herhangi bir iletişim ortamı üzerinden *kaplama (overlay)* ağ veya ikinci katman kontrol mekanizmalarına gerek kalmadan uçtan uca devre kurulmasını sağlar.

Geleneksel *IP* yönlendirmeli bir ağda *IP* paketi ağ üzerinde iletilirken bir *yönlendirici*ye uğradığında *yönlendirici*, paketin *IP* paket başlığındaki hedef adrese bakarak hedefe ulaşabilmesi için paketin bir sonraki durağını belirler. Bu belirleme işlemi için bir yönlendirme algoritması çalıştırılır. Hedefe varıncaya kadar her yeni durakta aynı işlemler tekrarlanır. *MPLS* ağlarda ise paket, *MPLS* ağına girdiğinde paket başlığı okunur ve ikinci ve üçüncü katman başlıklar arasına *MPLS* başlığı eklenir. Bu başlık içerisinde paketin bundan sonraki rotasını belirleyecek olan etiket bulunur. Paket her yeni durağında geliş portu ve etiketi göz önünde bulundurularak var olan etiketi çıkartılıp yeni etiketi eklendikten sonra bir sonraki durağına iletilir. Yönlendirme kararlarının etikete bakılarak yapılması hız dışında paket tabanlı bir altyapıya deterministik devre anahtarlama imkânı getirerek ağ üzerinde daha fazla kontrol sağlar. Etiketler otomatik olarak veya operatör tarafından elle atanabilir.



Şekil 1: MPLS genel etiket şekli [13].

3.1. MPLS ve Güvenlik

Güvenlik açısından baktığımızda *MPLS*'in trafik mühendisliği (*TE*), servis kalitesi (*QoS*), performans garantisi (*CoS*), tünel oluşturma, *VPN* teknolojisi ile birlikte kullanılabilme avantajları ve felaket yönetimi (*disaster recovery*) gibi nedenlerden dolayı ölçeklenebilirlik ve yüksek erişebilirlik sağlayarak dolaylı olarak ağa güvenlik sağlar. Buna rağmen güvenlik, *MPLS*'in en önemli geliştirme nedeni değildir ve temel *MPLS* mimarisi güvenlik hizmeti sağlamaz. Artan *MPLS* kullanımı ile birlikte *MPLS* ağları için güvenlik beklentilerinin artması araştırmacılar ve servis sağlayıcıları güvenlik için çeşitli alternatifler aramaya itti ve bunun sonucunda bazı yaklaşımlar ortaya atıldı. Bu yaklaşımlardan biri *VPN* ile *MPLS*'in beraber kullanılma durumudur.

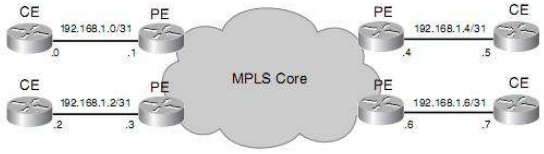
3.2. MPLS-VPN

MPLS, etiket-adresleme mantığı sayesinde *VPN* kullanımı için etkili bir yöntem sunmaktadır. *MPLS*'in *etiket yığıtlama* (*label stacking*) mantığıyla *MPLS* ağ üzerinde her *VPN* için farklı tüneller oluşturulabilir. Trafiğin bu şekilde ayrılması bir *VPN*'e ait trafiğin sadece o *VPN* içinde kalmasını sağlar. *MPLS-VPN* ağında çekirdek ağa giriş noktası *PE (Provider Edge)* denilen uç *yönlendirici*dir. Her *VPN* için bağlantı *CE (Customer Edge)* olarak adlandırılan bir *yönlendirici*yle sağlanır (bkz. *Şekil 2*). *PE-CE* eşleşmesi, çekirdek ağa olan tek erişim noktası olması nedeniyle *PE yönlendirici* en yüksek

güvenlik özellikleriyle korunmalıdır. Sadece *PE yönlendirici*nin dışarıdan görülebilmesi nedeniyle *MPLS* çekirdek ağın yapısı da saklanmış olur. Bir *PE yönlendirici*ye birden fazla *CE yönlendirici* bağlanarak bir *PE* üzerinden birden fazla *VPN* çekirdek *MPLS* ağa bağlanabilir. Fakat tavsiye edilen durum her *PE* için bir *CE* eşleşmesi olmasıdır. Güvenliğin arttırılması için *PE-CE* arasında Firewall kullanılabileceği gibi ulaşım kontrol listesi (*ACL*) veya paket filtreleme ile veya eşleştiği *CE yönlendirici* ile *MD5 (Message Digest)* kimlik doğrulama (*authentication*) yaparak korunabilir. Bu şekilde hizmeti engelleme (*DoS*) ataklarına karşı daha güvenli hale gelir. Ayrıca güvenlik sebebiyle *PE yönlendirici*lerin *CE yönlendirici*lerden gelen ve etiket içeren paketleri iptal etmesi gerekir. *CE yönlendirici*ler *MPLS* ağın dışında kaldığı için etiket ekleme durumunda değildir ve etiket içeren bir paketin gelmesi muhtemel bir saldırı olabilir.

Aynı fiziksel ağın farklı *VPN*'ler tarafından paylaşılması adreslerin tekil ve yönlendirme tablolarının farklı olmasını gerektirir. Farklı *VPN*'ler arasında adres tekilliğinin sağlanması *VPN-IP* adresleri tarafından sağlanır. *VPN-IPv4* adresleri 8 *byte* rota ayırıcı ve 4 *byte IP* adresi içerir. Bu adresler aynı zamanda özel adresler de olabilir [12]. *MPLS* bu şekilde her bir *VPN* için farklı adres uzayları oluşturarak adres tekilliği sağlar. Yönlendirme tablolarının farklı olmasını ise her *PE yönlendirici*nin kendisine bağlı her *VPN* için farklı bir sanal yönlendirme iletme (*VRF- Virtual Routing Forwarding*) tablosu tutması sağlar. *VPN* rotalarının dağıtılması için *MP BGP (Multi Protocol Border Gateway Protocol)* kullanılması önerilmiştir. Bu şekilde *BGP* bilgileri çekirdek ağa değil sadece diğer *PE yönlendirici*lere dağıtılır. Ve bu *yönlendirici*ler üzerinde her *VPN* için *VRF* tablosu oluşturulur. Böylece yönlendirme işlemi her *VPN* için ayrılmış olur.

MPLS-VPN daha çok servis sağlayıcılar tarafından sağlanır ve *VPN* kullanımında bir ağın birden fazla şirket tarafından kullanılması söz konusu olduğundan her ne kadar bir şirketin ağ üzerindeki bilgisinin sadece o şirkete ait *VPN* üzerinde dolaşacağı temin edilse de *MPLS-VPN* şifreleme ve mahremiyet sağlamaz. *MPLS*'in şifreleme sağlamaması nedeniyle *MPLS-VPN*'in çekirdek ağ içinde kullanımı uygundur ve uzaktan bağlantılar için *IPSec* ile birlikte kullanım tercih edilmelidir.



Şekil 2: MPLS-VPN mimari örneği şekli [14].

3.3. MPLS-VPN-IPSec

MPLS, VPN ile kullanılsa da şifreleme hizmeti olmadığı için mahremiyet garantisi sağlayamaz. Bu yüzden *MPLS-VPN* ile birlikte *IPSec* tünelleri kullanılmalıdır. *IPSec* kullanımı ile ağ üzerindeki trafik şifrelendiği için verinin mahremiyeti sağlanır. Veri alışverişinde bulunan iki uç nokta arasında kimlik doğrulama yapılır ve bu sayede paketin ağ üzerinde değişikliğe uğramayacağı garanti edilerek veri bütünlüğü sağlanmış olur. Eski veya tekrar eden paketleri tespit ederek bunları reddeder ve tekrar gönderim ataklarına karşı güvenlik sağlar.

MPLS ve *IPSec*'in birlikte kullanılması *VPN*'ler için yüksek seviyede güvenlik sağlar.

3.4. OSI Modeli ve Diğer Olası Güvenlik Açıkları

OSI referans modeli ağ protokolleri dizaynında referans alınan katmanlı tanımlamadır. Güvenlik modeli oluştururken muhtemel saldırıları için *OSI* referans modelinin kullanılması saldırıların farklı katmanlar için modellenmesini dolayısıyla da bunlar için alınabilecek tedbirlerin daha kolay hazırlanmasını sağlayabilir. Makalemizde *MPLS* kullanımı ile birlikte ağ güvenliği ele alınsa da *MPLS* daha önce de belirttiğimiz gibi tek başına güvenlik sağlamamaktadır ve güvenlik için ek teknolojiler gerekmektedir. Bu teknolojileri sadece eş ve üstü katmanlar olarak görmeyip tüm *OSI* katmanlarının gözden geçirilmesi olası güvenlik sorunlarının tespitinde bize kolaylık sağlayacaktır. Şöyle ki sosyal mühendislik yöntemi kullanılarak elde edilebilecek bir şifrenin hangi network protokolünün altyapıda kullanılmasıyla bir alakasının olmadığı gibi fiziksel katmana kazma kürekle yapılabilecek en amatör bir saldırının da uygulama katmanında bir *kerberos* yönteminin kullanılması fayda etmeyecektir. Bu bölümdeki amacımız her katmanı ayrı değerlendirerek olası güvenlik riskleri için o katmanda etkin güvenlik çözümünün bulunmasıdır.

3.4.1. Fiziksel Katman

Diğer saldırıların aksine genelde fiziksel katmana yapılan saldırıların çoğu basit veya çok az bilgi gerektirir. Sinyali kesme saldırıları bu kapsamda değerlendirilebilir. Veri iletişiminin çoğunun yerin birkaç metre altından geçen kablolarla veya kablosuz istasyonlarla sağlandığı düşünüldüğünde basit yöntemlerle kablolara zarar verilebilir veya sinyal karıştırıcılarla kablosuz iletişim kalitesi düşürülebilir veya tamamen verimsiz hale getirerek etkisizleştirilebilir. Geniş bant ağ kablolarının geçtiği noktalar yanlışlıkla kazı yapılmasının önüne geçilmesi için genellikle endüstrice bilinir. Birkaç sene önce Türk Telekom satışı sürecinde yaşanan ve daha çok fiber optik kablolara özellikle de Türk Telekom personeli tarafından kolayca yapılan saldırılar aslında güvenliğin ne kadar kolay bir şekilde yerle bir edilebileceğini göstermesi bakımından ilginçtir. Ayrıca zaman zaman okyanus altından geçen kablolarda yaşanan kopmalar uzun süreli hizmet kesintilerine yol açmakta ve sabotaj kuşkusu yaratmaktadır. Bu konunun öneminin anlaşılması ve özellikle askeri ve kritik öneme sahip enerji ve bankacılık alanları için kullanılan iletişim hatlarının geçtiği noktaların gizli tutularak azami güvenlik özellikleriyle inşa edilmesi ve olağanüstü durumlar için alternatif iletişim hatlarının bulundurulması konusunda daha fazla çalışma yapılmalıdır. Ayrıca okyanus altından geçen veri iletim kablolarının veri iletimi esnasında meydana getirdiği manyetik alandan etkilenen köpek balıklarının veri iletim kablolarına yaptığı saldırılar sonucunda veri iletim kablolarında meydana gelen hasarın önüne geçilebilmesi için veri iletim kablolarının tasarımında yeni yaklaşımlara ihtiyaç vardır. Veri iletim kablolarının çevreye daha az etki edecek şekilde üretilmesi

hem çevreye hem de kendi kullanım ömrüne dolayısıyla da veri taşınan hattın güvenliğine olumlu yönden etki edecektir.
Paket izleme fiziksel katmanda yapılabilecek bir diğer saldırı türüdür. Ağı izlemede kullanılan ağ monitör araçlarının mantığıyla paketlerin izlenmesi ve içeriğinin elde edilmesi önemli bir güvenlik zafiyetidir. Çeşitli üst katman yöntemleriyle paket içerikleri şifrelense bile elde edilebilecek bilgiler diğer saldırılara yol açabilir. Paket içeriğinden çok paket trafiğinin yoğunluğu ve istikametine göre kritik bir sunucunun hangisi olduğu ortaya çıkabilir ve bu bilgi kullanılarak *hizmeti kesme* (*DoS*) dâhil olmak üzere diğer saldırı türlerine sebebiyet verebilir.

3.4.2. Veri İletim Katmanı

Veri iletim katmanı fiziksel katmandan aldığı ham veriyi *frame* haline getirir ve hedef adres olarak *MAC (Media Access Control)* adreslerini kullanır. *MAC* adresleri bir üst katman olan network katmanının anlayabildiği adres türü olan *IP* adresine *ARP (Address Resolution Protocol)* protokolü ile çevrilir. *MAC-IP* adres eşlenikleri ön bellekte tutulur ve tabloda bulunmayan bir *IP* adresi için ağa *ARP* sorgusu gönderilir ve gelen cevaba göre önbelleğe bu *MAC-IP* eşleşmesi atılır. Buradaki sorun *ARP* protokolünün evresiz (*stateless*) olmasından dolayı herhangi bir istek gelmese de ARP cevabı olarak bir bilgisayara yanlış bir *MAC-IP* eşleniği gönderilebilir ve bilgisayar da bu bilgiyi ön belleğine kaydeder. Ayrıca ağ üzerindeki *anahtarlayıcı*lara (*switch*) belleği doluncaya kadar yanlış *MAC* bilgisi göndererek *anahtarlayıcı*ların gelen tüm trafiği doğrudan ağa vermesine neden olacak şekilde bir saldırı gerçekleştirilebilir.

3.4.3. Network Katmanı

Ağ katmanında ağ üzerinde paketlerin hareketini sağlayan *IP* protokolü çalışır. Her ağın iletim katmanının türüne bağlı olarak taşıyabileceği maksimum paket büyüklüğü *MTU* ile belirlenmiştir. Ethernet için bu 1500 *byte*dır. Bu büyüklüğü geçen paketler parçalara ayrılarak taşınır. Bu parçalar hedef adrese geldiğinde tekrar birleştirilir. Bu parçalardan sadece ilki protokol başlığını taşır. Her bir parçanın başlığında ise ofset, uzunluk gibi bilgiler bulunur ki bu bilgiler değiştirilerek bölütleme (*fragmentation*) atağı yapılabilir. *ICMP (Internet Control Message Protocol)* mesajları ile kaynak adres değiştirilerek kurbanın adresi yazılır ve tüm ağa *echo* sorgusu yollanarak ağ üzerinden yüksek sayıda cevap gelmesi sağlanır. Bu şekilde kurban işleyemeyeceği kadar mesaj alır. Ağ ve kurban bilgisayar işlemez duruma getirilir. Normalde iletişim için kullanılmayan alanların zarar verme amaçlı veri konulabilir. *ICMP echo* içine isteğe bağlı olarak veri konulabilir. Genellikle bunların kontrolü yapılmaz. *MPLS* ağlar içinde de *ICMP* mesajları kullanılabilmektedir. [15]

3.4.4. Diğer Katmanlar

Diğer katmanlara yönelik hizmetin kesilmesi (*DoS*), işletim sistemine yönelik ataklar, kimlik denetimini aşmaya yönelik ataklar, virüsler, solucanlar, truva atları ve kullanıcıya yönelik ataklar sayılabilir.

4. Tartışma

Her ne kadar *MPLS* kullanımının artmasıyla beraber *MPLS* ağlarda güvenliği sağlayacak yeni yaklaşımlar geliştirilse de hala *MPLS* sinyal ve kontrol sisteminin güvenliğini sağlarken ölçeklenebilirlik ve esnekliğin korunabilmesine yönelik çözümler bulunamamıştır. Ayrıca *MPLS* ağların çekirdek kısmının *VPN* kullanımında özellikle içeriden yapılabilecek ataklarda *VPN* kullanıcılarına yeterli güvenlik sağlayamadığı ortadadır. *IPSec* kullanımı ile yüksek bir güvenlik sağlanabilse de bu durumda da ölçeklenebilirlik ve esneklik azalmaktadır. Özellikle *VoIP* uygulamaları için *IPSec* kullanımı şifreleme başlığının ses paketlerine eklenmesi sonucunda seslerin karşı tarafa kesik kesik ve anlaşılamaz bir şekilde gitmesine neden olabilir.

5. Sonuçlar

MPLS her ne kadar performans, esneklik, ölçeklenebilirlik, hizmet kalitesi gibi değerler sunsa da güvenliğin *MPLS*'in esas geliştirme hedefi olmaması nedeniyle yüksek güvenlik sağlayacak yaklaşımlar kullanıldığında *MPLS*'in ölçeklenebilirlik, esneklik gibi özelliklerinden uzaklaşıldığı görülmüştür. Şu anda optimum çözümün *MPLS-VPN* kullanımı olduğu görülmektedir. Daha yüksek güvenlik sağlayabilmek için her *PE* üzerinden sadece bir *VPN*'in çekirdek *MPLS* ağa bağlanması, her *PE-CE* eşleşmesi için *firewall*, ulaşım kontrol listeleri ve *PE-CE* arasında *statik IP* kullanılmalıdır. Farklı *VPN*'ler arasında trafik akışı olmayacağı garanti edilse bile çekirdek *MPLS* ağa içeriden yapılabilecek saldırılara karşı çok yüksek güvenlik beklentileri varsa *IPSec* de mimariye eklenmelidir. Doğru çözümün bulunabilmesi için ihtiyaçların iyi analiz edilmesi gerekmektedir. İhtiyaçlar iyi analiz edildikten sonra *MPLS* diğer rakiplerine göre en uygun çözümü sunmaktadır.

6. Kaynakça

[1] Johnson, C. B. , ``MPLS and MPLS VPNs: Basics for Beginners'', *http://www.infosecwriters.com/text_resources/pdf/CJohnson_MPLS_VS_MPLS_VPN.pdf*

[2] E. Rosen, A. Viswanathan, and R. Callon, "Multi-protocol Label Switching Architecture", *IETF, RFC 3031, 2001.*

[3] Cisco Systems White Paper, "Security of the MPLS Architecture", *http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/mxinf_ds.pdf*, August 2001.

[4] Rosen, E. and Y. Rekhter. , "BGP/MPLS VPNs", *IETF RFC 2547, March 1999.*

[5] Muthukrishan, K. and A. Malis, "A Core MPLS IP VPN Architecture", *IETF RFC 2917, September 2000.*

[6] Cisco Systems White Paper, "Analysis of MPLS-Based IP VPN Security: Comparison to. Traditional l2VPNs such as ATM and Frame Relay, and. deployment guidelines", *http://www.cisco.com/warp/public/cc/so/neso/vpn/prodlit/mpvpn_wp.pdf*, March 2004.

[7] D. Grayson, et al., "Analysis of security threats to MPLS virtual private Networks", *International Journal of Critical Infrastructure Protection (2009), doi:10.1016/j.ijcip.2009.08.002*

[8] Palmieri F. and Fiore U. , “Enhanced security strategies for MPLS signaling”, *JOURNAL OF NETWORKS, VOL. 2, NO. 5, SEPTEMBER 2007*

[9] Spainhower M. , Butts J. , Guernsey D. , Shenoi S. , “Security analysis of RSVP-TE signaling in MPLS networks”, *International Journal of Critical Infrastructure Protection (2008), doi:10.1016/j.ijcip.2008.08.005*

[10] Alouneh S. , En-nouaary A. , Agarwal A. , " A Multiple LSPs Approach to Secure Data in MPLS Networks", *JOURNAL OF NETWORKS, VOL. 2, NO. 4, AUGUST 2007*

[11] Schneider F. B. , "CS 5430 System Security - Introduction", Lecture Notes, *http://www.cs.cornell.edu/courses/cs5430/2009sp/paper.chptr01.pdf*

[12] Y. Rekhter , Moskovitz B. , et. al. “Address Allocation for Private Internets“, *IETF RFC 1918, February 1996.*

[13] “Multi-Protocol Label Switching (MPLS) Conformance”, *http://www.abc188.com/info/html/wangluozhishi/wangluoxieyi/20080224/28793_2.html*

[14] Froom R. , Sivasubramanian B. , Frahim E. , “CCNP Self-Study: Building Cisco Multilayer Switched Networks, 3rd Edition” , http://searchnetworking.techtarget.com/searchNetworking/Downloads/CCNP_BCMSN_ch3.pdf

[15] Bonica R. , D. Gan. , “ICMP Extensions for MultiProtocol Label Switching“, *IETF RFC4950, August 2007.*