İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

OPTİK WDM AĞLARINDA HATA BAĞIŞIKLIĞININ SAĞLANMASI İÇİN PROTOKOL

YÜKSEK LİSANS TEZİ

Müh. Hülya HOCAOĞLU

Anabilim Dalı: Bilgisayar Mühendisliği

Programı: Bilgisayar Mühendisliği

Tez Danışmanı: Yrd. Doç. Dr. Feza BUZLUCA

MAYIS 2005

ÖNSÖZ

Tez çalışmam boyunca, her zaman yapıcı olan önerileriyle bana verdiği şevk, destek ve anlayışı için tez danışmanım Yrd. Doç. Dr. Feza BUZLUCA'ya en içten teşekkürlerimi sunuyorum. Lisans ve yüksek lisans öğrenimim boyunca kendisinden ders alma fırsatına sahip olmaktan ve kendisi gibi işine değer veren, saygı duyan ve her şeyden önce işini seven birini tanımaktan ötürü kendimi şanslı gördüğümü özellikle vurgulamak istiyorum. Kendisinin şahsında, öğrenim hayatım boyunca bana inanan ve destek olan tüm öğretmenlerime teşekkür ediyorum.

Kendimi kötü hissettiğim zamanlarda benden desteklerini esirgemedikleri ve beraber geçirdiğimiz – ve geçireceğimiz – tüm güzel zamanlar için dostlarıma teşekkür ediyorum.

En derin ve özel teşekkürlerim AİLEME; her zaman yanımda oldukları, anlayışları, sabırları, güvenleri ve hayata gülen gözlerle bakmayı öğrettikleri için.

Mayıs 2005 **Hülya HOCAOĞLU**

İÇİNDEKİLER

KISALTMALAR

ATM	: Asynchronous Transfer Mode
GMPLS	: Generalized Multi Protocol Label Switching
IP	: Internet Protocol
LDP	: Label Distribution Protocol
LMP	: Link Management Protocol
LOL	: Loss of Light
LOS	: Loss of Signal
LSP	: Label Switched Path
MPLS	: Multi Protocol Label Switching
OSPF-TE	: Open Shortest Path First-Traffic Engineering
OTN	: Optical Transport Network
OXC	: Optical Cross Connect
RSVP-TE	: Resource Reservation Protocol-Traffic Engineering
SDH	: Synchronous Digital Hierarchy
SONET	: Synchronous Optical Network
SRLG	: Shared Risk Link Group
TCP	: Transmission Control Protocol
WDM	: Wavelength Division Multiplexing

TABLO LİSTESİ

ŞEKİL LİSTESİ

Sayfa No

SEMBOL LİSTESİ

G	:Ağın fiziksel topolojisini gösteren grafik
N	:Ağda yer alan düğümler. 1'den N'ye kadar numaralandırılmışlardır
F	:Ağda yer alan fiberler. 1'den F'ye kadar numaralandırılmışlardır
W	:Bir fiberdeki iletişim için kullanılabilecek dalgaboyu sayısı
S	:Ağa veri pompalayan kaynak düğümler
D	:Verinin gönderilmek istendiği hedef düğümler

OPTİK WDM AĞLARINDA HATA BAĞIŞIKLIĞININ SAĞLANMASI İÇİN PROTOKOL

ÖZET

Bilgisayar ağlarında taşınan veri trafiğinin – özellikle Internet'in dünya çapındaki yaygın kullanımından kaynaklanan – hızlı artışı ile birlikte, veri odaklı bilgisayar ağlarının çalışır durumda tutulması para, zaman ve iş gücü kaybının önlenmesi açısından giderek daha karmaşık ve önemli hale gelmektedir. Optik WDM ağlarının sunduğu çok büyük bant genişliğinden dolayı bu ağlarda meydana gelen çok kısa süreli bozulmalar dahi dramatik sonuçlara neden olabilmektedir.

Bilgisayar ağlarında hata bağışıklığının sağlanması uzun yıllardır araştırılan bir konudur. Ağların çalışır durumda tutulması için izlenen başlıca iki yaklaşım vardır: koruma (protection) ve onarma (restoration). Koruma, statik bir yöntem olarak addedilebilir. Bu yöntemde kaynaklar (fiber kablolar, dalga boyları, cihazlar, vs), ağ oluşturulurken yedeklenir. Korumanın en önemli avantajı hatalara çok hızlı cevap verebilmesidir ki bu, optik WDM ağları için hayati öneme sahiptir. Öte yandan, yedeklenen kaynaklar ağ ömrünün büyük bölümünde atıl durumda bulunduğundan ağ verimli kullanılmamaktadır.

Onarma ise dinamik bir yaklaşım izler; dolayısıyla ağ kaynakları daha etkin biçimde kullanılır. Bu yöntemde çözüm, problem oluştuktan sonra bulunmaya çalışılır. Veri akışının sağlanacağı yeni yolların bulunması ve kurulmasının zaman alması onarmanın zayıf yönünü ortaya çıkarır: hatalara cevap vermede korumaya göre olan görece yavaşlık.

Günümüzde SONET-ATM tabanlı ağların yerini IP tabanlı ağlar almaktadır. Bu geçişte üstesinden gelinmesi gereken en önemli problem, servis kalitesinin sağlanması ve hataları düzeltme hızının SONET ağlarıyla rekabet edebilecek seviyeye getirilmesidir. Bu amaçla, özellikle MPLS ve GMPLS'in geliştirilmesiyle birlikte hata bağışıklığı getirmeyi amaçlayan çeşitli protokoller ortaya çıkmıştır.

Bu tez çalışmasında, hata bağışıklığı konusunda bugüne kadar yapılmış olan çalışmaları geliştiren ve hataların hangi katmanda ve ne şekilde çözüleceğine karar veren bir yönetici hata bağışıklığı protokolü geliştirilmiştir. Protokolün geliştirilmesinde, değişikliklere uyum sağlayabilen dinamik yapısından dolayı onarma yöntemi benimsenmiştir. Protokol, hataları sezme ve düzeltme konusunda halihazırda var olan yöntemlerden yararlanmaktadır.

A PROTOCOL FOR PROVIDING SURVIVABILITY IN OPTICAL WDM NETWORKS

SUMMARY

Along with the rapid growth in the data traffic, mainly because of the widespread use of the Internet, managing data-centric networks and maintaining them in working state has become more complex and more important in means of data, time, and revenue. Because of the huge bandwidth and speed they provide, fast restoration and high survivability is of crucial importance for optical networks.

Providing survivability in computer networks has been an area of research for long years. Two main approaches are followed for maintaining networks at working state: protection and restoration. Protection can be considered as a static method. Resources (which can be bandwidth, wavelength channels, lightpaths, labelpaths, OXCs, etc) are backed up while the network is provisioned. The advantage of this method is to provide very fast recovery which is vital in order to prevent loss of data. On the other hand, the network is not fully utilized since back up resources are not used for the most of the time.

Due to its dynamicity, restoration is more effective in utilizing the network. In this approach, a new way to transport the data is found after the fault occurs. However, since calculating a new route is a time consuming process, restoration methods respond more slowly to faults.

Nowadays, IP based OTNs are replacing SONET-ATM based networks. At this transition, the most challenging problem is providing QoS and being able to cope with the very short response times to faults of SONET rings. Especially with the evolution of MPLS and GMPLS, new protocols for providing survivability are being developed and the existing ones are enhanced.

In this study, a management protocol, which is targeted to unify and enhance the previous work on survivability area and solve the problem at the most suitable layer and within a very short period of time, is developed. The protocol adopts the restoration method for dynamicity and better utilization. It takes advantage of the existing protocols for detecting faults and recovery.

1. GİRİŞ

Günümüzde Internet, her meslek grubundan insanın iş ve günlük hayatında kullandığı kritik bir yapı halini almıştır. Bankacılık işlemlerinden elektronik postaya, elektronik alışverişten bilimsel araştırmalara kadar insan hayatının pek çok alanında vazgeçilmez bir yardımcı konumundadır. Internetin dışında, büyük veya küçük pek çok kuruluş adanmış hatlar vasıtasıyla iş görmektedir. Bu hatlar kurumun farklı şehirler, farklı ülkeler, hatta farklı kıtalardaki merkezlerini birbirine bağlamak ya da çalışanların işyerine dahi gelmeden bilgisayarları aracılığıyla bu hatlara bağlanarak çalışmalarını sağlamak gibi değişik amaçlar için kullanılmaktadır. Tüm bu sebeplerden dolayı bilgisayar ağlarında taşınan veri miktarı da üstel bir biçimde artmaktadır.

Teknolojinin ucuzlaması ile birlikte bilgisayar ağlarında optik altyapının kullanımı yaygınlaşmıştır. Fiber optik kablolar bakır ve benzeri diğer iletim ortamlarına kıyasla çok büyük hız ve bant genişliği sağlamaktadır. Bu hız ve bant genişliğine erişilmesinde en önemli katkıyı, WDM teknolojisinin ve OXC'ler gibi çok yüksek kapasiteli anahtarlama aygıtlarının geliştirilmesi sağlamıştır. Bu sayede, tek bir fiberden çok kısa sürede çok büyük miktarda veri iletilebilmektedir (tek bir fiber üzerinden 1 Tb/s). Tüm bunlar göz önüne alındığında, bir optik ağda çok kısa süreli bir bozulma ya da servis dışı kalmanın ne kadar büyük miktarda veri kaybına sebep olacağı kolayca anlaşılır.

Haberleşme ağlarının (önceleri ses daha sonra veri, görüntü, vb. taşıyan) ortaya çıkışından itibaren bu ağların işler durumda tutulması, üzerinde çalışılan bir konu olmuştur. Geleneksel yöntemler, kaynakların yedeklenmesine dayanır. Ağın planlanması aşamasında, oluşturulan iletişim hatları için bu hatların bozulması durumunda devreye girecek yedek hatlar da oluşturulur. Hata durumlarında müdahaleler genellikle sistem yöneticileri tarafından elle yapılır.

Ancak zamanla, haberleşme ağlarının çok büyümesi ve giderek daha karmaşık hale gelmesi insan eliyle yapılacak müdahaleleri kabul edilemez hale getirmiştir. Özellikle WDM teknolojisinin kullanıldığı ağlarda mümkün olan en kısa sürede hataları çözmek ve ağı bütünüyle çalışır duruma getirmek gerek işgücü, gerek para, gerekse prestij kaybını önlemek için elzemdir.

Bu noktadan hareketle, ağlarda hata bağışıklığını sağlamak için çeşitli yöntemler geliştirilmiştir. Bu yöntemlerin temel amaçları; hataları sezmek, yalıtmak ve nihai hedef olarak düzeltmektir. İki temel yaklaşım vardır: koruma ve onarma. Bu yöntemlerin çalışma prensipleri ve birbirlerine olan üstünlükleri ileride ayrıntılandırılacaktır. Yöntemlerin, hataları hangi katmanda sezeceği ve çözeceği konusunda da başlıca iki görüş savunulur. Bunlardan ilki, hatanın sezildiği katmanda çözülmesini – çözülebiliyorsa – öngörür. İkinci görüş ise hatanın sezildiği katmana en yakın ya da en uzak katmandan başlayarak çözülene kadar katmanlar arasında aşağı ya da yukarı ilerlemeyi hedefler. Ancak hangi ana ya da alt yöntem kullanılıyor olursa olsun, bağışıklığın sağlanması konusunda karar verici bir mekanizmanın eksikliği hissedilmektedir.

Bu tez çalışmasında, hata bağışıklığı konusunda yapılmış olan çalışmalar incelenmiş ve bunların faydalı yönlerini birleştirecek bir yöntem geliştirilmeye çalışılmıştır. Yöntem, kararların verileceği bir hata bağışıklığı yönetici protokolünü önerir. Hata bağışıklığı protokolü, değişimlere olan dayanıklılığından ötürü onarma yaklaşımını benimser. Hataların sezilmesi ve düzeltilmesi konusunda, hata bağışıklığı sağlamak için değişik katmanlar için geliştirilmiş protokollerden yararlanılır. Böylece, fiziksel, veribağı, ağ ve ulaşım katmanlarında hataların sezilmesi olanağına kavuşulur. Sezilen her hata, sezen katman (protokol) tarafından hata bağışıklığı yöneticisine bildirilir. Oluşan hatalar karşısında ne gibi önlemlerin alınacağını yönetici belirler. Bu sayede, hataların, yönetici tarafından verilen rasyonel kararlar doğrultusunda en uygun katmanda ve en kısa sürede çözülmesi sağlanır.

Bu çalışmadaki temel amaç, optik WDM ağlarında meydana gelen hataların mümkün olan en kısa sürede sezilmesi ve düzeltilmesidir. Bunun için çeşitli optimizasyonlar yapılmıştır.

Bir sonraki bölümde, hata bağışıklığı konusunda geliştirilmiş yöntemler, çalışma prensipleri, üstün yanları ve eksikleri tanıtılmaktadır.

Üçüncü bölümde önerilen yöntem, yöntemin onarmayı hedeflediği hata tipleri, bu amaçla kullanılan protokoller ve çalışma şekli ayrıntılı olarak açıklanmıştır.

Dördüncü bölümde, benzetim programı ile ilgili açıklamalar ve elde edilen sonuçlar yer almaktadır.

Son bölüm, elde edilen sonuçları değerlendirerek yapılan çalışmayı özetler.

2. HATA BAĞIŞIKLIĞINA GENEL BAKIŞ

Bu bölümde optik ağlarda hata bağışıklığı konusu tanıtılmaktadır. Hata bağışıklığına neden ihtiyaç duyulduğu, hata bağışıklığı sağlanmasında kullanılan yöntemler, bu yöntemlerin eksi ve artı yönleri ve hata bağışıklığı alanında halihazırda var olan ihtiyaçlar tartışılmaktadır. Bölüm, okuyucuya tez boyunca işlenen konuyu anlayabilmesi için gerekli temel bilgileri sunmaktadır.

2.1 Hata Bağışıklığının Tanımı ve Gerekleri

Bilgisayar ağlarında hata bağışıklığı, ağın hatalara karşı dayanıklı olması, hata durumlarında verinin iletilebileceği alternatif yollar bulunabilmesi ve bu sayede, iletilen verinin sürekliliğinin sağlanması şeklinde tanımlanabilir. Optik ağlarda hatalar, anahtarlama aygıtlarında (OXC) ya da fiber hatlarda meydana gelmelerine göre iki sınıfa ayrılabilir. Fiber kablolarda meydana gelen hatalar genellikle fiber kesilmeleri gibi – özellikle karasal alanlarda – harici sebeplerden kaynaklanır. Aygıtlarda oluşan hatalar ise genellikle donanım problemleri ya da yazılım yetersizlikleri gibi iç nedenlere dayanır. Bunun dışında, güç sağlayıcılarda meydana gelen anomaliler, doğal felaketler ya da terörist saldırılar gibi dış nedenler de aygıt hatalarına neden olabilir. Şu ana kadarki tecrübeler, aygıt hatalarının iletim ortamı hatalarına oranla daha az görüldüğünü ortaya koymaktadır. Bununla birlikte, bir anahtarlama aygıtında oluşacak hata ilgili düğümden geçen tüm veri trafiğinin kesilmesine neden olacağından çok daha hayati sonuçlar doğurabilir [1, 2].

Haberleşme ağlarında hata bağışıklığının sağlanması için yapılan çalışmalar oldukça eski yıllara dayanmaktadır. Bu nedenle, haberleşme ağlarının elektronik katmanları için oldukça yerleşmiş koruma yöntemleri bulunmaktadır. Örneğin, SONET/SDH halkaları ve IP için hata bağışıklığı yöntemleri yaygın olarak kullanılmaktadır [1]. Her ne kadar bugün hala SDH/SONET veya ATM tabanlı IP ağları kullanılıyor olsa da, haberleşme teknolojisi, iletişim katmanlarının sayısını azaltarak doğrudan WDM üzerinde çalışacak IP yapılanmasına doğru yol almaktadır [13]. Bundan dolayı, WDM katmanı için, 1 Tb/s gibi son derece yüksek hızlarda taşınan veriler için oluşan

hataları kompanze edebilecek kadar etkin hata bağışıklığı yöntemlerinin geliştirilmesi gerekmektedir.

WDM katmanında hata bağışıklığı sağlanmasını tetikleyici nedenler şu şekilde sıralanabilir:

- Bir hatanın, meydana geldiği katmanda düzeltilmesi tercih edilir.
- WDM'de yapılacak hata düzeltmelerle hataların SDH/SONET katmanındakinden daha kısa sürede çözülmesi hedeflenmektedir. (SDH/SONET için bu süre 60-100 ms arasındadır) [1].
- Hataların mümkün olduğu kadar alt katmanlarda sezilmesi ve düzeltilmesiyle, üst katmanların ağ ile ilgili ayrıntılı bilgi sahibi olma yükümlülüğü ve gerekliliği azalır.

Farklı katmanlar için çalışan değişik hata bağışıklığı mekanizmaları bulunmasına rağmen, bu katmanlardaki işlemleri koordine edecek ve yapılması gereken işlemlerle ilgili kararları verecek bir yönetici katman ile ilgili çalışmalar son derece sınırlıdır. [3] ve [12], bu konuya değinen nadir çalışmaları içermektedir.

2.2 Hata Bağışıklığı Yöntemlerinin Sınıflandırılması

Haberleşme ağlarında hata bağışıklığı, dolayısıyla hizmet verme sürekliliğini sağlamak için kullanılan yöntemler, koruma ve onarma olmak üzere iki temel sınıfa ayrılır.

2.2.1 Koruma Yöntemi

Bu yöntemde yedek kaynaklar, çağrının kurulması sırasında, hata durumlarında ilgili çağrı tarafından kullanılmak üzere tahsis edilir. Koruma yöntemine dayanan hata bağışıklığı şemaları, çağrının yönlendirilebileceği yedek kaynaklar ayrılmış olduğundan, hatalara çok kısa sürede cevap verirler. Öte yandan, yedekleme mantığına dayandıklarından, ağ kaynaklarının etkin kullanılmamasına sebep olurlar [4].

Koruma şemaları, birincil kaynak yedek kaynak eşleşme biçimine göre iki alt sınıfa ayrılabilir:

- Birebir eşleşme (1:1): Birebir eşleşmede her bir çağrı için bir birincil bir de hata durumunda kullanılacak yedek yol tahsis edilir. Yüzde yüz koruma sağlar; ancak kaynaklar son derece hor kullanılmış olur (kaynakların %50'si atıl durumdadır) [9].

- 1:n eşleşme: Bu yöntemde bir yedek kaynak birden fazla birincil kaynak tarafından paylaşılır. Birincil kaynaklarda meydana gelen herhangi bir hatada hepsi aynı yedek kaynağı kullanmak ister. Dolayısıyla, yedeği paylaşacak birincil kaynakların aynı senaryoda bozulmayacak şekilde seçilmeleri yani aynı risk grubu (SRLG) içinde yer almamaları gerekir. Paylaşılan koruma sayesinde kaynaklar nispeten daha verimli kullanılmış olur [1, 2, 4, 10].

Koruma şemaları için başka bir alt sınıflandırma, korunan birime göre yapılabilir:

- Yol koruma: Yol korumada, her bir çağrı için kurulan yolların bir de yedeği kurulur. Uçtan uca koruma sağlar.

- Hat koruma: Bu yöntemde yedekleme hat bazında yapılır. Çağrılar için oluşturulan yollar, bu korunan hatların peş peşe eklenmesiyle kurulur. Hat koruma, küçük parçalar için çalıştığından, hataları yol korumaya göre daha kısa sürede düzeltir. Bununla birlikte, yüksek bir hesaplama ve sinyalleşme yükü getirir [2].

2.2.2 Onarma Yöntemi

Onarma yönteminde temel yaklaşım şu şekildedir: Bir hata tarafından etkilenen çağrılar için, hata oluştuktan sonra, yeni yollar hesaplanır ve çağrılar bu yollara yönlendirilir. Onarmanın en önemli avantajı esnekliğidir. Yedek kaynakların birkaç hata senaryosu için paylaşılmasına imkan verir. Bunun sonucu olarak da ağ kaynakları etkin bir biçimde kullanılmış olur. Onarma yönteminin eksi yönü ise, yol hesaplanması ve kurulmasının getirdiği yükten dolayı, düzeltme süresinin korumaya göre daha uzun olmasıdır [5].

2.3 GMPLS İçin Hata Bağışıklığı

GMPLS'nin bilgisayar ağları dünyasına getirdiği en önemli yeniliklerden biri çeşitli servis kalitelerinde, trafik mühendisliği yapılabilen çağrıların otomatik olarak kurulabilmesidir. Halen yaygın olarak kullanılmakta olan ve haberleşme ağlarının temelini oluşturan SONET halkalarında, çağrı için yol kurulması, elle yapıldığından, uzun süren ve maliyetli bir işlemdir. GMPLS tabanlı ağların kullanılması bazen aylar sürebilen bu kurulum işlemini dakikalar mertebesinde bir süreye indirebilecektir [6].

2.3.1 GMPLS'de Yol Kurulumu

GMPLS için kurulan yollar Label Switched Path (Etiket Anahtarlamalı Yol) olarak adlandırılmaktadır. LSP'lerin otomatik olarak kurulabilmesi için ağdaki her düğümde bir Label Distribution Protocol (Etiket Dağıtım Protokolü) çalışmaktadır. En yaygın kullanımı olan Etiket Dağıtım Protokolü RSVP-TE'dir. Bu, standart RSVP protokolünün trafik mühendisliği yapılabilecek şekilde geliştirilmiş bir versiyonudur. Kaynak düğümler, protokolün PATH mesajını kullanarak yeni bir ışıkyolu (LSP) kurma isteğinde bulunurlar. Kurulan yollarla ilgili olarak RSVP-TE'nin sağladığı özellikler aşağıda sıralanmıştır [7, 8].

- Servis kalitesi sağlayacak biçimde LSP oluşturulması
- Kurulmuş olan LSP'lerin dinamik olarak yeniden yönlendirilmesi
- Bir LSP'nin gerçekte kullandığı yolun gözlemlenebilmesi
- LSP'lerin hata için incelenebilmesi

Bu tez çalışmasında, ışıkyollarının kurulması için RSVP-TE protokolünden yararlanılmaktadır. Yol kurulumunda kullanılan PATH mesajının formatı Şekil 2.1'de verilmiştir [7].

<Path Message> ::= <Common Header> [<INTEGRITY>]

<SESSION> <RSVP_HOP>

<TIME VALUES>

[<EXPLICIT_ROUTE>]

<LABEL_REQUEST>

[<SESSION ATTRIBUTE>]

[<POLICY DATA> ...]

<sender descriptor>

<sender descriptor> ::= <SENDER TEMPLATE> <SENDER_TSPEC>

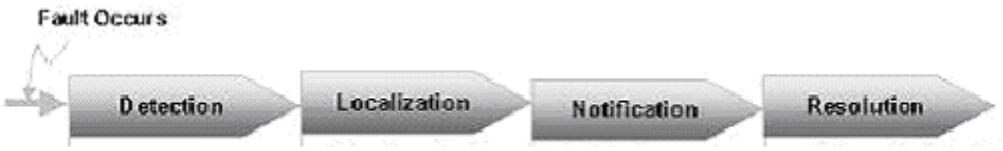
[<ADSPEC>]

[<RECORD_ROUTE>]

Şekil 2.1 RSVP-TE PATH mesajı formatı

2.3.2 GMPLS Hata Bağışıklığı Mekanizması

GMPLS'nin temel özelliklerinden bir diğeri hata yönetimini de otomatikleştirmesidir. Şekil 2.2'de hata yönetimindeki temel adımlar gösterilmiştir.



Şekil 2.2 GMPLS için hata yönetimi adımları [6]

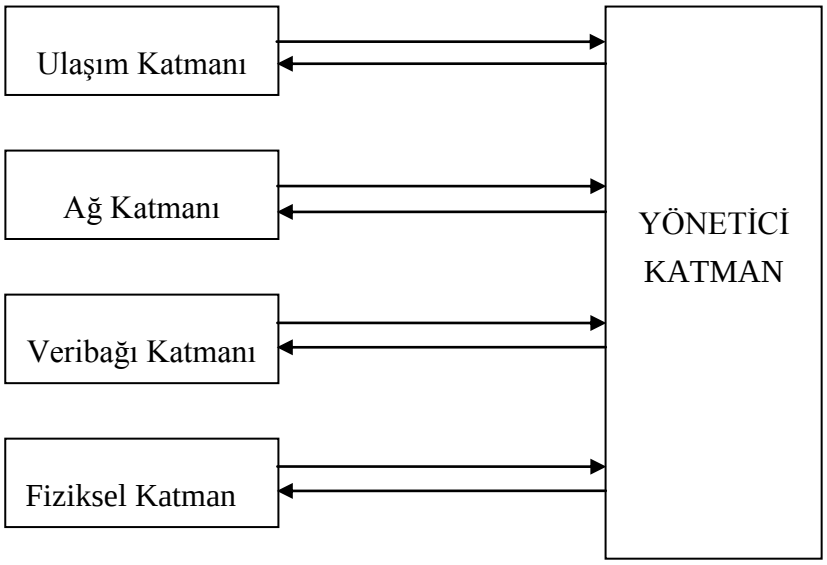
GMPLS, iki komşu düğüm arasında yer alan hatlar ya da uçtan uca LSP'ler için olmak üzere iki farklı seviyede onarma sağlayabilmektedir. Hat bazlı onarmada, yeni yol hatayı sezen ara düğüm tarafından kurulur. Uçtan uca hata bağışıklığı için ise, bir hata durumunda yeni yol kurma talebinde kaynak düğüm bulunur.

Bu çalışmada, hataları sezmek ve topolojideki değişikliklerden haberdar olabilmek için GMPLS protokol ailesinde yer alan OSPF-TE [8, 9] ve LMP [10,] protokolleri kullanılmıştır.

3. HATA BAĞIŞIKLIĞI İÇİN YÖNETİCİ PROTOKOL

Bu çalışmadaki temel amaç, hata durumlarında onarma için yapılacak işlemlere karar veren bir hata bağışıklığı yönetici protokolünü tasarlamaktır. Hata bağışıklığı protokolü, oluşan tüm hatalardan haberdar olmak ve yapılacak onarma işlemlerini bildirmek üzere fiziksel katman, veribağı katmanı, ağ katmanı, ulaşım katmanı ve GMPLS protokolleri ile iletişim kurabilmektedir. Oluşan her hata, kendisini sezen katman (protokol) tarafından, hemen hata bağışıklığı yönetici protokolüne bildirilir. Yönetici protokol, hatayı inceledikten sonra, gerekli işlemleri bu işlemleri yürütmesini istediği katmana bildirir. Protokol, kaynak keşfi, yol kurulumu ve hata sezme için bu amaçlarla geliştirilmiş diğer protokollerden yararlanır.

Hata bağışıklığı yönetici katmanının diğer katmanlarla olan ilişkisi Şekil 3.1'de görülebilir.



Şekil 3.1 Hata bağışıklığı protokolünde katmanlar arası ilişki

3.1 Tanımlar ve Varsayımlar

Hata bağışıklığı protokolünü geliştirmek için kullanılan notasyon şu şekilde tanımlanmaktadır:

- *G:* Ağın fiziksel topolojisini gösteren grafik
- *N:* Ağda yer alan düğümler. 1'den N'ye kadar numaralandırılmışlardır
- *F:* Ağda yer alan fiberler. 1'den F'ye kadar numaralandırılmışlardır
- *W:* Bir fiberdeki iletişim için kullanılabilecek dalgaboyu sayısı
- *S:* Ağa veri pompalayan kaynak düğümler
- *D:* Verinin gönderilmek istendiği hedef düğümler

Protokol şu varsayımlar altında geliştirilmiştir:

- Trafik matrisi zaman içinde değişmez. Yani S (kaynak düğümler) ve D (hedef düğümler) kümeleri sabittir.
- Her bir fiberde kullanılabilecek W (dalgaboyu sayısı) sabittir ve bu sayı ağda yer alan tüm fiberler için aynıdır.
- Ağdaki her düğüm bir OXC ve IP yönlendirici ile donatılmıştır.
- Tüm OXC'ler herhangi bir dalgaboyunu başka herhangi bir dalgaboyuna çevirebilirler.
- Yönetici katman; fiziksel katman, veribağı katmanı, ağ katmanı, ulaşım katmanı ve GMPLS protokolleri ile doğrudan iletişim kurabilmektedir.
- Hata bağışıklığı yönetici protokolü sadece kaynak düğümlerde çalışmaktadır. Dolayısıyla hataların sezilmesi ve düzeltilmesinden kaynak düğümler sorumludur.
- Ağ çapında, tüm kaynak düğümlerde çalışan hata bağışıklığı yönetici protokolleri birbirleriyle haberleşebilmektedir.

3.2 Sezilebilen ve Onarılabilen Hatalar

Hata bağışıklığı yönetici protokolü, Tablo 3.1'de yer alan hataları sezmeyi ve onarmayı hedeflemektedir.

Tablo 3.1 Sezilebilen ve onarılabilen hatalar

HATA	SEZEN PROTOKOL
Yerel cihazda hata	LOL
Komşu cihazda hata	LMP
Ara fiberde hata	LOL, LMP
Ağa fiber hat eklenmesi	LMP, OSPF, Hata bağışıklığı yönetici protokolü rapor mesajı
Ağdan fiber hat çıkarılması	LMP, OSPF, Hata bağışıklığı yönetici protokolü rapor mesajı
Ağa düğüm eklenmesi	LMP, OSPF, Hata bağışıklığı yönetici protokolü rapor mesajı
Ağdan düğüm çıkarılması	LMP, OSPF, Hata bağışıklığı yönetici protokolü rapor mesajı
Ulaşım katmanı hatası	TCP

Tablo 3.1'de de görüldüğü gibi hataların sezilmesinde var olan protokollerden yararlanılmıştır. Bu protokollerin nasıl kullanıldığı Bölüm 3.3.'te açıklanacaktır.

Ağ topolojisinin tamamını bilmek ve ağda meydana gelen değişikliklerden haberdar olmak için OSPF-TE protokolü kullanılmaktadır. Bu protokol, çalıştığı her düğümde, ağda yer alan tüm düğümlerin birbirleriyle olan bağlantılarını gösteren bir tablo tutmaktadır. OSPF tablosu, gene OSPF protokolü tarafından güncellenmektedir. Ancak, bilindiği gibi, OSPF protokolünün yakınsama süresi uzun olabilmektedir. Dolayısıyla, ağ topolojisinde meydana gelen bir değişikliğin tüm düğümler tarafından öğrenilmesi, optik WDM ağlarında hataları sezmek için kabul edilemeyecek kadar uzun olabilmektedir. Bu nedenle, önerilen protokolde OSPF tablosu, güncel tutulabilmesi amacıyla, yönetici katmanın istekleri doğrultusunda da güncellenebilmektedir. Bu şekilde, hata sezme ve onarma süresinin kısaltılması hedeflenmiştir.

Ağ topolojisinin yanı sıra, yönetici protokol, kendi düğümünden kaynaklanan veri akışları için kurulan ışıkyollarının hangi düğüm ve fiberlerden geçtiğini de bilmek zorundadır. Bunun için her kaynak düğümde bir *Işıkyolu Tablosu* tutulmaktadır. Bu tablonun yapısı Tablo 3.2'de verilmiştir.

Tablo 3.2 Işıkyolu tablosu

IŞIKYOLU NO	HEDEF	YOL
1	N2	N4 F2 N5 F4 N3 F1 N2

3.3 Hata Sezme ve Yol Kurulumu İçin Kullanılan Protokoller

Bu tez çalışması, bilgisayar ağlarında hata bağışıklığı alanında yapılmış olan çalışmalardan yararlanarak, hata bağışıklığı sağlanması için gerekli işlemleri -düğüm bazında- koordine edecek bir yönetici katman önermektedir. Bu doğrultuda, hataları sezme ve onarma için halihazırda var olan protokoller kullanılmaktadır.

Farklı hata tipleri farklı katmanlar tarafından sezilebilmektedir. Bir hatanın, sezilebileceği en alt katmanda, dolayısıyla en kısa sürede sezilmesi amaçlanmıştır. Sezilen her hata, hata bağışıklığı yönetici katmanına bildirilmekte ve onarma için ne yapılması gerektiğine yönetici katman karar vermektedir.

İzleyen bölümlerde, hata bağışıklığı sağlanmasında katmanlar arasındaki görev dağılımı anlatılmıştır.

3.3.1 Fiziksel Katman

Fiziksel katman iki farklı hata tipini sezebilmektedir:

- Yerel cihazın iletişim arayüzlerinde meydana gelen hatalar
- Düğüme doğrudan bağlı olan fiber hatlarda meydana gelen hatalar

Yerel cihazda meydana gelen hatalar için hata bağışıklığı protokolünün sağlayabileceği herhangi bir düzeltme yoktur. Bundan dolayı, cihaz doğrudan iletişime kapatılmaktadır.

Doğrudan bağlı olan fiber hatlarda meydana gelen hatalar, fiziksel katmanda LoL (Işık Kaybı) veya LoS (İşaret Kaybı) protokolleri tarafından sezilmektedir. Bu tip bir hatayı sezen fiziksel katman, hemen hatanın meydana geldiği fiberi yönetici katmana bildirmektedir. Bu noktada fiziksel katmanın sorumluluğu biter. Onarma için ne yapılacağı konusunda söz, yönetici katmandadır.

Bölüm 1'de anlatıldığı gibi, bilgisayar ağlarında hatalar genellikle iletim ortamlarında meydana gelmektedir. Böyle bir durumda, sorunun hızla ortadan kaldırılabilmesi için, fiber hatlarda meydana gelen hataların fiziksel katman tarafından sezilmesi önemlidir. Böylece, üst katmanlar hatadan etkilenmeden ve en az veri kaybıyla hata onarılabilir. Buradan yola çıkılarak, hata bağışıklığı yönetici protokolünün çalışma döngüsünde, fiziksel katman tarafından bildirilen hataların işlenmesine öncelik verilmiştir.

3.3.2 Veribağı Katmanı

Veribağı katmanı tarafından sezilmesi beklenen değişiklikler ve hatalar şunlardır:

- Komşu cihazda meydana gelen hatalar
- Yeni bir komşunun eklenmesi veya var olan bir komşunun çıkarılması
- Doğrudan bağlı fiber hatlarda meydana gelen hatalar
- Yeni bir fiberin doğrudan bağlanması veya doğrudan bağlı bir fiberin sökülmesi

Bu değişiklikleri sezmek için veribağı katmanı, LMP (Bağlantı Yönetim Protokolü) protokolünden yararlanır. OSPF protokolünün Bölüm 3.2'de de bahsi geçen nispeten uzun yakınsama süresinden dolayı, komşu cihazlarda meydana gelen hataları (veya ekleme/çıkarma gibi değişiklikleri) ilk öğrenecek birim, LMP protokolü vasıtasıyla veribağı katmanıdır. Dolayısıyla, onarma süresinin kısaltılabilmesi için, LMP tarafından hataların sezilebilmesi ve hızla yönetici katmana bildirilmesi oldukça önemlidir.

Doğrudan bağlı bir fiber hat bozulduğunda, çıkarıldığında ya da yeni bir fiber eklendiğinde, veribağı katmanı hangi hattın bozulduğu ya da yeni hattın nereye eklendiği bilgilerini yönetici katmana iletir. Aynı değişiklikler düğümler için söz konusu olduğunda da hangi düğümün bozulduğu veya eklenen düğümün bağlantı bilgileri yönetici katmana bildirilir.

Veribağı katmanının hata sezme dışındaki bir diğer sorumluluğu, yönetici katmandan gelen direktifler doğrultusunda yeni ışıkyollarının kurulmasıdır. Işıkyolları RSVP-TE protokolu vasıtasıyla kurulur. Yol kurulumu için gönderilen Path mesajına, RECORD_ROUTE nesnesi eklenerek ışıkyolunun geçtiği düğüm ve fiberlerin

kaynak düğüm tarafından bilinmesi sağlanır [7]. Işıkyolu tablosunda saklanan bu bilgiler, yönetici katman tarafından karar verme aşamasında kullanılmaktadır.

3.3.3 Ağ Katmanı

Ağ katmanı, OSPF-TE protokolü vasıtasıyla ağ topolojisini öğrenir ve OSPF tablosunda saklar. Topolojide herhangi bir değişiklik meydana geldiğinde, OSPF tablosu güncellenir ve meydana gelen değişiklik hata bağışıklığı yönetici katmanına bildirilir.

Hata bağışıklığı yönetici protokolünün doğru ve hızlı çalışabilmesi için ağ topolojisinin en son halini bilmesi büyük önem arz etmektedir. Bazen uzak bir düğümde meydana gelen bir hatanın OSPF protokolü ile tüm ağa bildirilmesi çok uzun zaman alabilir. Bu da, hatanın oluştuğu düğümü kullanarak ya da o düğüme veri gönderen düğümler için önemli veri kayıplarına sebep olur. Bu istenmeyen durumu önlemek için, Bölüm 3.3.1 ve 3.3.2'de açıklandığı gibi, bazı hataların yerel olarak daha alt katmanlarda sezilmesine çalışılır. Fiziksel katman ve veribağı katmanı tarafından sezilen bu hatalar yönetici katmana bildirildikten sonra, yönetici OSPF-TE'den herhangi bir bildirim olmamasına rağmen, OSPF tablosunun güncellenmesine karar verebilir. Tüm bu çabalar, ağ topolojisi bilgisinin sürekli güncel tutulması içindir.

3.3.4 Ulaşım Katmanı

Bu katman tarafından yönetici katmana bildirilebilecek hatalar, TCP protokolünün standart hatalarıdır [11]. Gerçekte, hata bağışıklığı yönetici protokolünün doğru çalışması durumunda, ulaşım katmanından herhangi bir hata bildirilmemesi beklenmektedir. Çünkü, bir hatanın, ulaşım katmanını etkileyecek kadar ilerlemesinden önce, daha alt katmanlar tarafından yöneticiye bildirilmiş ve düzeltilmiş olması amaçlanmıştır. Dolayısıyla, TCP tarafından bildirilen hatalar, yönetici protokolün ya da hata sezme mekanizmalarının doğru çalışıp çalışmamasıyla ilgili bir uyarı niteliği taşıyabilir ve önerilen protokolün sağlamlık teyidi için kullanılabilir.

3.4 Çalışma Yöntemi

Hata bağışıklığı için yönetici protokol, ağa veri pompalayan kaynak düğümlerde çalışmak üzere tasarlanmıştır. Dolayısıyla, ağda meydana gelen hataları sezmek ve onarmak kaynak düğümlerin sorumluluğudur. Bir kaynak düğüm, sezdiği her hata için onarma girişiminde bulunmaz. Kaynaklar, hatayı onarma sorumluluğunun kendilerine ait olup olmadığına şu kıstaslara göre karar verirler:

- Meydana gelen hata, ilgili düğümden kaynaklanan veri akışlarından en az birini etkiliyorsa, kaynak onarma için harekete geçer.
- İlgili kaynağın veri akışları hatadan etkilenmiyorsa diğer kaynak düğümlere sezdiği hatayı bildirmekle yetinir.

Kaynaklar, diğer düğümlerde ya da iletim hatlarında oluşan hatalardan etkilenip etkilenmediklerini anlamak için kendilerinden kaynaklanan veri akışları için kurulan ışıkyollarının, hatalı düğüm ya da fiberi kullanıp kullanmadıklarını bilmek zorundadırlar. Bunun için, her kaynak düğüm ışıkyollarının geçtiği fiziksel yolu gösteren bir *Işıkyolu Tablosu* tutar (Bkz. Tablo 3.2). Hatalardan etkilenen ışıkyolları yeniden yönlendirildiğinde, geçtikleri yeni yolu belirtmek üzere Işıkyolu Tablosu da güncellenir.

Etkilenen kaynak, onarma işlemini tamamladıktan sonra sezdiği hatayı ağda yer alan ve hata bağışıklığı yönetici protokolünün koştuğu diğer kaynak düğümlere de bildirir. Bu raporlama yöntemi ile, tüm kaynakların hatalardan mümkün olduğu kadar hızlı haberdar edilmesi amaçlanmıştır.

Hatayı sezen kaynak, bu hatadan etkilenmiyorsa sadece raporlama işlemini yürütür. Meydana gelen hata ağdaki hiçbir kaynak düğümün veri akışını etkilemiyorsa, bir yeniden yönlendirme yani onarmaya da gerek yok demektir. Dolayısıyla, ağın yeni durumunu bildirmek için bir rapor mesajı gönderilmesi yeterli olacaktır.

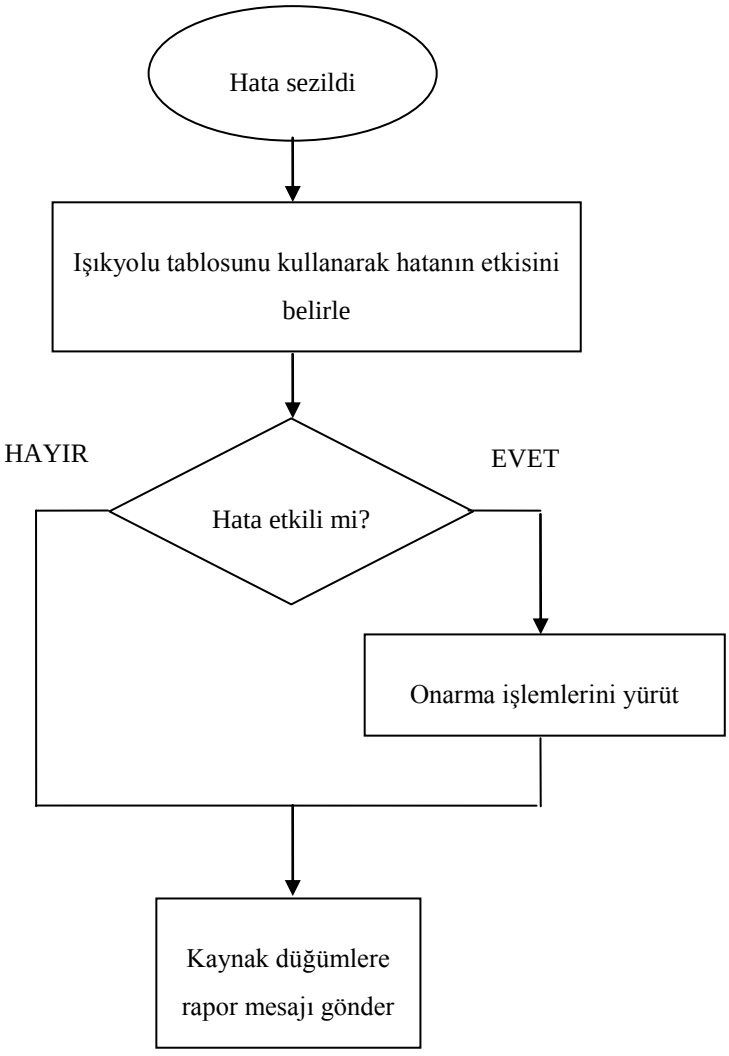
3.4.1 Onarma İşlemlerinin Hatalara Göre Sınıflandırılması

Bir hata ya da ağ topolojisinde bir değişiklik (fiber ya da düğüm ekleme ya da çıkarma gibi) sezen kaynak düğümün, hatanın tipinden bağımsız olarak, yürüteceği ilk adım hatanın kendi ışıkyollarına olan etkisini belirlemektir. Eğer hatanın ya da değişikliğin kendisi için etkisiz olduğuna karar verirse onarma işlemini, etkilenen kaynak düğümlere bırakır.

Hata ya da değişikliğin tipinden bağımsız olarak yürütülecek bir diğer işlem, bunun diğer kaynaklara bildirilmesidir. Bir kaynak düğüm, gerekli olduğuna karar verirse öncelikli olarak onarma işlemlerini yürütür, ardından rapor mesajını gönderir. Onarma işlemlerinin kendisi için gereksiz olduğuna karar verirse, diğer kaynak düğümleri bilgilendirerek oluşan hata ya da değişiklik ile ilgili işini bitirir.

Yönetici protokol, ağda meydana gelen bir değişikliği OSPF-TE protokolü aracılığıyla öğrenmişse, rapor mesajı göndermez. OSPF-TE, oluşan değişikliği tüm ağa yayacağından aynı hatayı bildiren iki mesajın ağda dolaşması önlenmiş olur.

Yukarıdaki paragraflarda anlatılan adımlar Şekil 3.2'de görülebilir.



Şekil 3.2 Hata tipinden bağımsız işlemler

Tüm hata ve değişiklikler için ortak olan bu iki işlem dışında, hata bağışıklığı yönetici protokolünün onarma amacıyla yürüttüğü işlemler, ağda meydana gelen

hatalara veya değişikliklere göre farklılık gösterir. Bölüm 1'de bahsedildiği gibi, bilgisayar ağlarında hatalar iletim hatlarında ve cihazlarda oluşmalarına göre iki ana grupta toplanabilir. Bölüm 3.4.1.1 ve 3.4.1.2.'de bu iki tip hata durumunda yürütülen işlemler açıklanmaktadır.

3.4.1.1 İletim Hatlarında Meydana Gelen Hatalar ve Değişiklikler

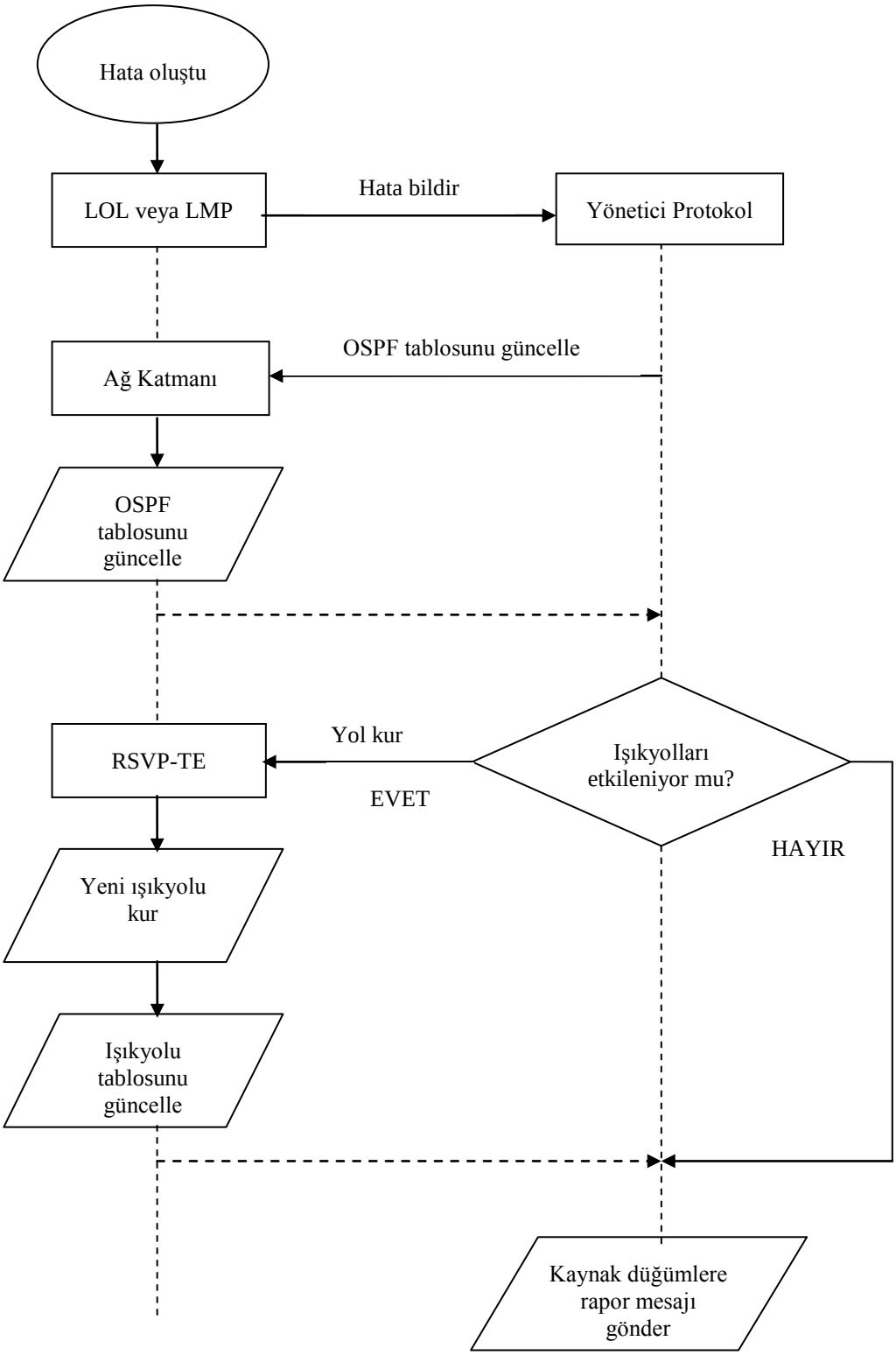
Bu grup, bilgisayar ağlarında en sık görülen hataları içerir. İletim hattı hataları sınıfında toplanabilecek hatalar ve değişiklikler ve bunlarla başa çıkabilmek için hata bağışıklığı yönetici protokolünün gerçekleştirdiği işlemler aşağıdaki gibi sınıflandırılabilir.

- Doğrudan bağlı fiberde hata oluşması;
    - LOL veya LMP protokolleri tarafından yöneticiye bildirilir.
    - Ağ katmanına OSPF tablosunu güncelleme isteği gönderilir.
    - Işıkyolu Tablosu kontrol edilerek, kaynağın ışıkyollarından herhangi birinin hatalı fiberden geçip geçmediği belirlenir.
    - Hatalı fiberi kullanan bir ışıkyolu varsa, buradaki veri akışının yeniden yönlendirilmesi için GMPLS'ye yeni ışıkyolu kurma isteği iletilir.
        - RSVP-TE protokolü kullanılarak yeni ışıkyolu kurulur ve veri akışı buraya yönlendirilir.
        - Işıkyolu tablosu güncellenir.
    - Hata kaynağın veri akışlarını etkilemiyorsa, bir onarma girişiminde bulunulmaz.
    - Oluşan hata, rapor mesajı ile diğer kaynak düğümlere bildirilir.
- Ağa fiber hat eklenmesi;
    - Eklendiği yere bağlı olarak, LMP, OSPF-TE veya rapor mesajı ile yönetici protokole bildirilir.

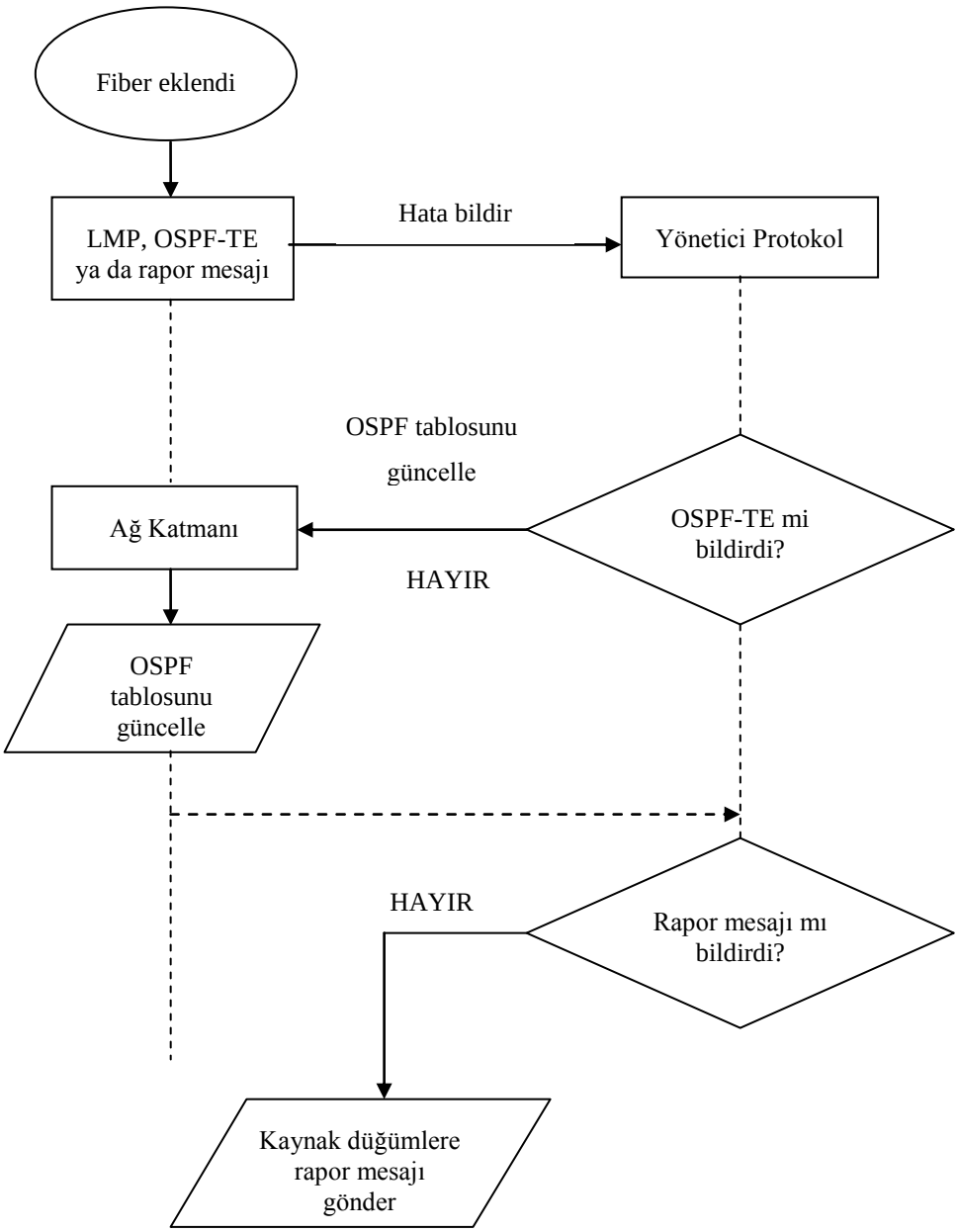
- OSPF-TE tarafından bildirilmediyse, zaman kaybını önlemek için, ağ katmanına OSPF tablosunu güncelleme isteği gönderilir.
- Değişiklik, OSPF-TE ya da rapor mesajı aracılığıyla öğrenilmediyse, diğer kaynak düğümlere bildirilir.

- Ağdan fiber hat çıkarılması
  - OSPF-TE ya da rapor mesajı ile yönetici protokole bildirilir.
  - OSPF-TE tarafından bildirilmediyse, zaman kaybını önlemek için, ağ katmanına OSPF tablosunu güncelleme isteği gönderilir.
  - Işıkyolu Tablosu kontrol edilerek, kaynağın ışıkyollarından herhangi birinin çıkarılan fiberden geçip geçmediği belirlenir.
  - Çıkarılan fiberi kullanan bir ışıkyolu varsa, buradaki veri akışının yeniden yönlendirilmesi için GMPLS'ye yeni ışıkyolu kurma isteği iletilir.
    - RSVP-TE protokolü kullanılarak yeni ışıkyolu kurulur ve veri akışı buraya yönlendirilir.
    - Işıkyolu tablosu güncellenir.
  - Hata kaynağın veri akışlarını etkilemiyorsa, bir onarma girişiminde bulunulmaz.
  - Değişiklik, OSPF-TE ya da rapor mesajı aracılığıyla öğrenilmediyse, diğer kaynak düğümlere bildirilir.

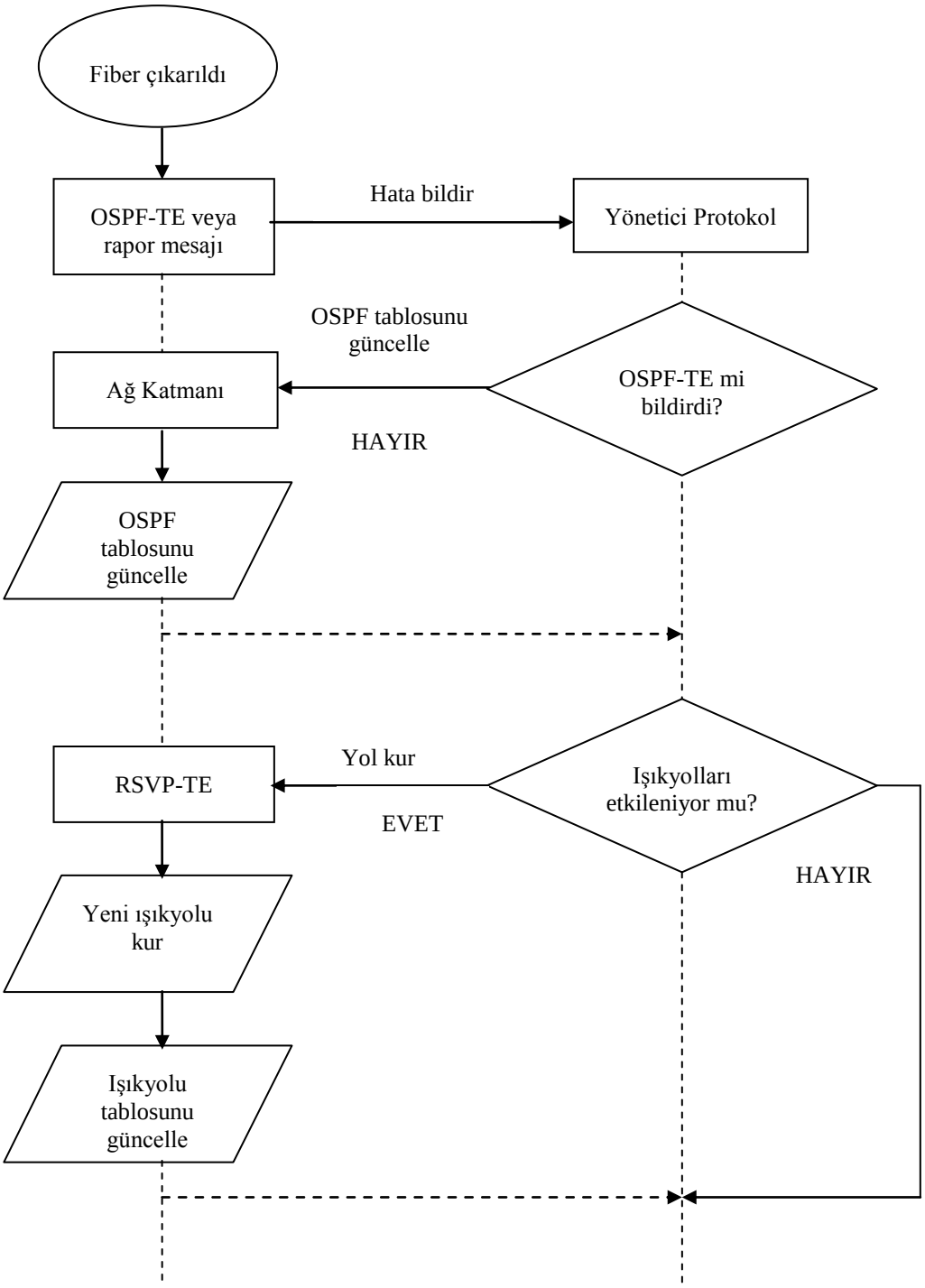
Bu durumlarda yürütülen işlemler Şekil 3.3, Şekil 3.4 ve Şekil 3.5'te gösterilmiştir.



Şekil 3.3 Doğrudan bağlı fiberde hata oluşması



Şekil 3.4 Ağa fiber hat eklenmesi



Şekil 3.5 Ağdan fiber hat çıkarılması

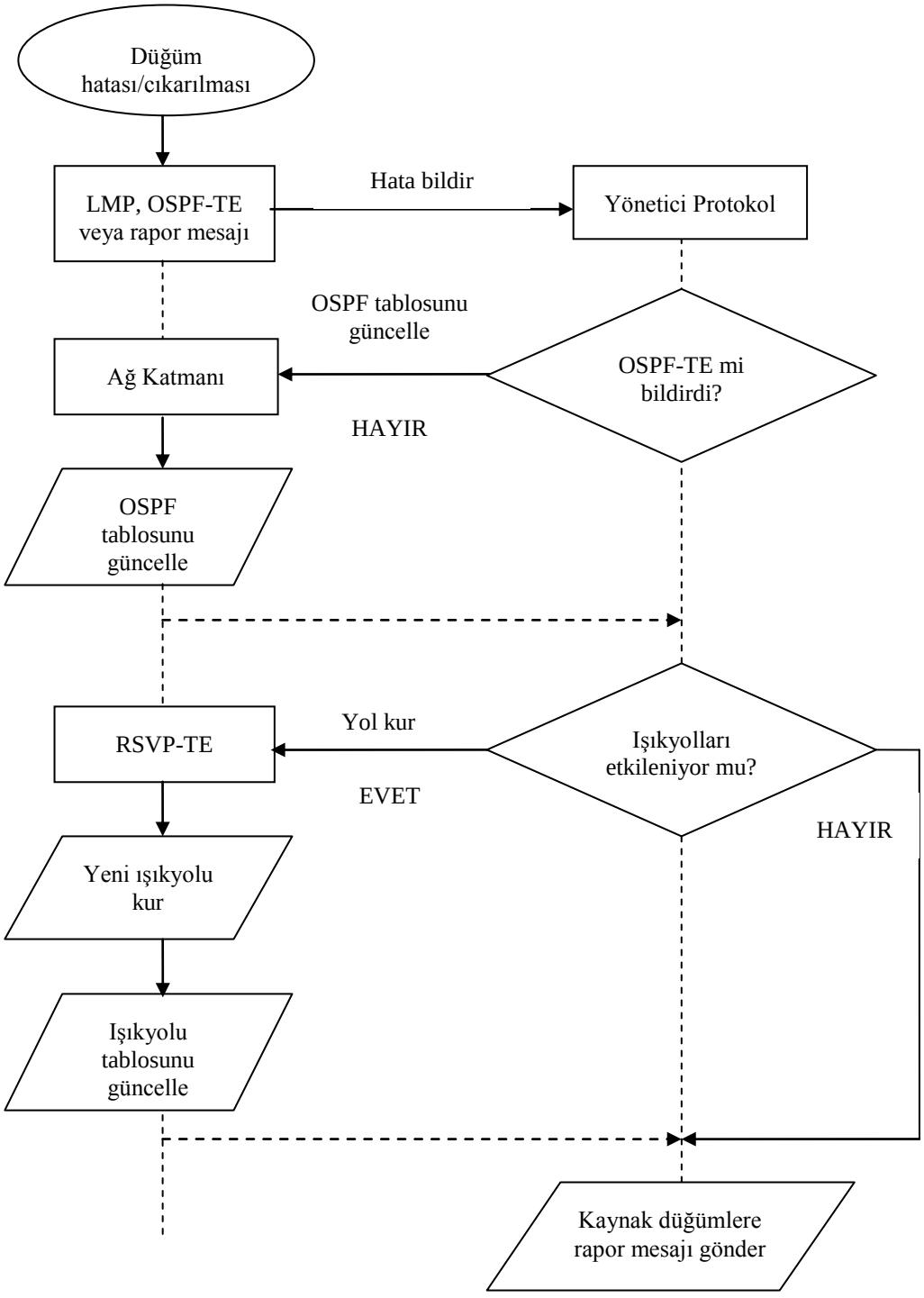
3.4.1.2 Ağda Yer Alan Düğümlerde Meydana Gelen Hatalar ve Değişiklikler

Bilgisayar ağları için iletişim aygıtlarında yani düğümlerde hata görülme sıklığı, iletim hatlarına oranla daha düşüktür. Bununla beraber, bir düğümde meydana gelen hata o düğümden kaynaklanan veya geçen tüm veri trafiğini etkileyeceğinden, bu sınıfta yer alan hatalar çok dikkatle yönetilmelidir.

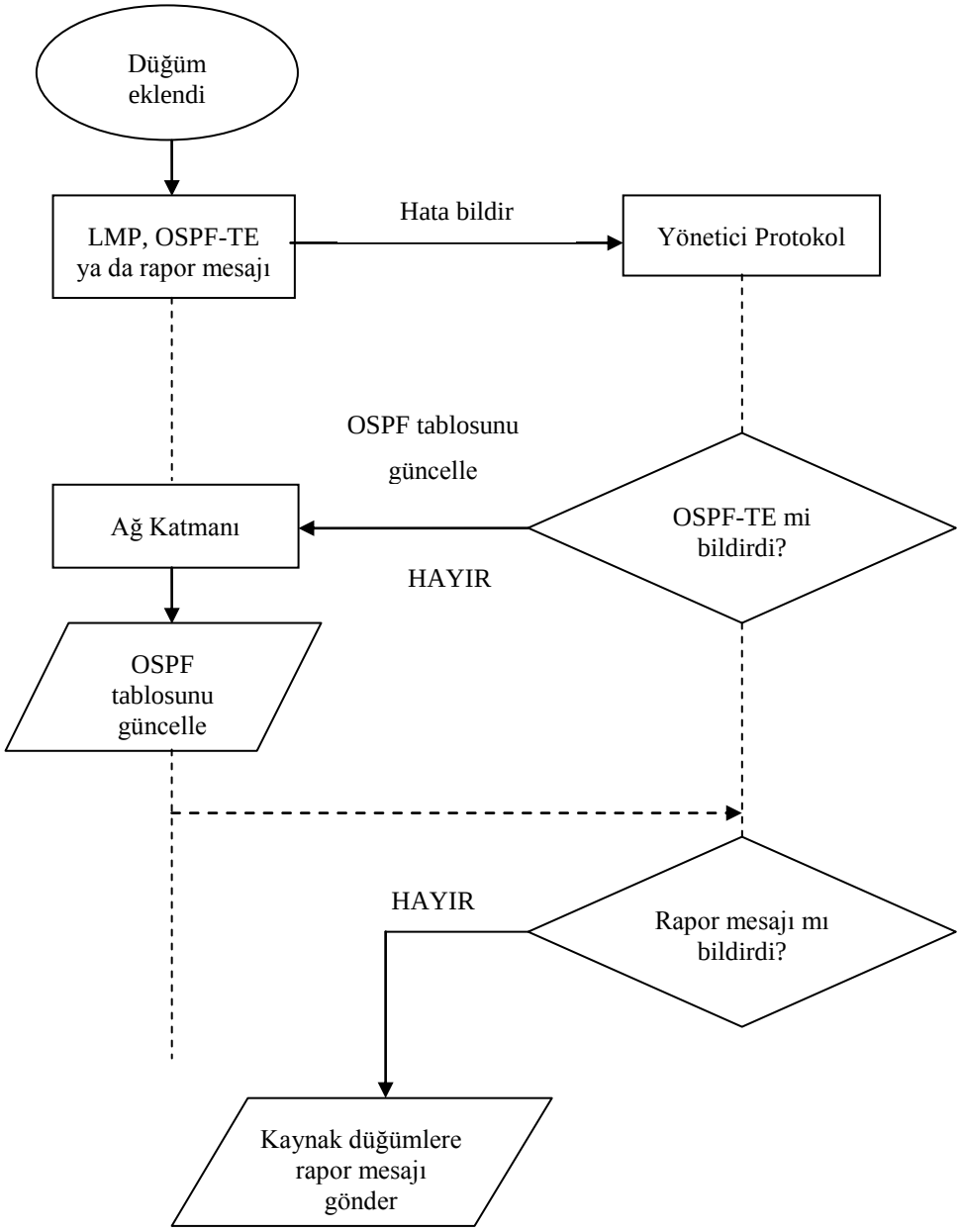
Bu tür hatalarda hata bağışıklığı yönetici protokolünün izlediği yol, aşağıda açıklanmıştır.

- Bir düğümde hata oluşması ya da bir düğümün ağdan çıkarılması;
    - Hatalı ya da çıkarılan düğümün yerine bağlı olarak, LMP, OSPF-TE veya rapor mesajı ile yöneticiye bildirilir.
    - Ağ katmanına OSPF tablosunu güncelleme isteği gönderilir.
    - Işıkyolu tablosu kontrol edilerek, kaynağın ışıkyollarından herhangi birinin hatalı veya çıkarılan düğümden geçip geçmediği belirlenilir.
    - Hatalı veya çıkarılan düğümü kullanan bir ışıkyolu varsa, buradaki veri akışının yeniden yönlendirilmesi için GMPLS'ye yeni ışıkyolu kurma isteği iletilir.
        - RSVP-TE protokolü kullanılarak yeni ışıkyolu kurulur ve veri akışı buraya yönlendirilir.
        - Işıkyolu tablosu güncellenir.
    - Hata kaynağın veri akışlarını etkilemiyorsa, bir onarma girişiminde bulunulmaz.
    - Oluşan hata, rapor mesajı ile diğer kaynak düğümlere bildirilir.
- Ağa düğüm eklenmesi;
    - Eklendiği yere bağlı olarak, LMP, OSPF-TE veya rapor mesajı ile yönetici protokole bildirilir.
    - OSPF-TE tarafından bildirilmediyse, zaman kaybını önlemek için, ağ katmanına OSPF tablosunu güncelleme isteği gönderilir.
    - Değişiklik, OSPF-TE ya da rapor mesajı aracılığıyla öğrenilmediyse, diğer kaynak düğümlere bildirilir.

Bu iki durumda yürütülen işlemler, Şekil 3.6 ve Şekil 3.7'de gösterilmiştir. Bunlar, iletim hattı hataları için yürütülen işlemlere benzerdir. Ancak, yönetici katman ile diğer katmanlar arasında gidip gelen mesajlar farklılık gösterir. Hata bağışıklığı yönetici protokolünün kullandığı mesaj yapısı ve mesaj tipleri, Ek A'da gösterilmiştir.



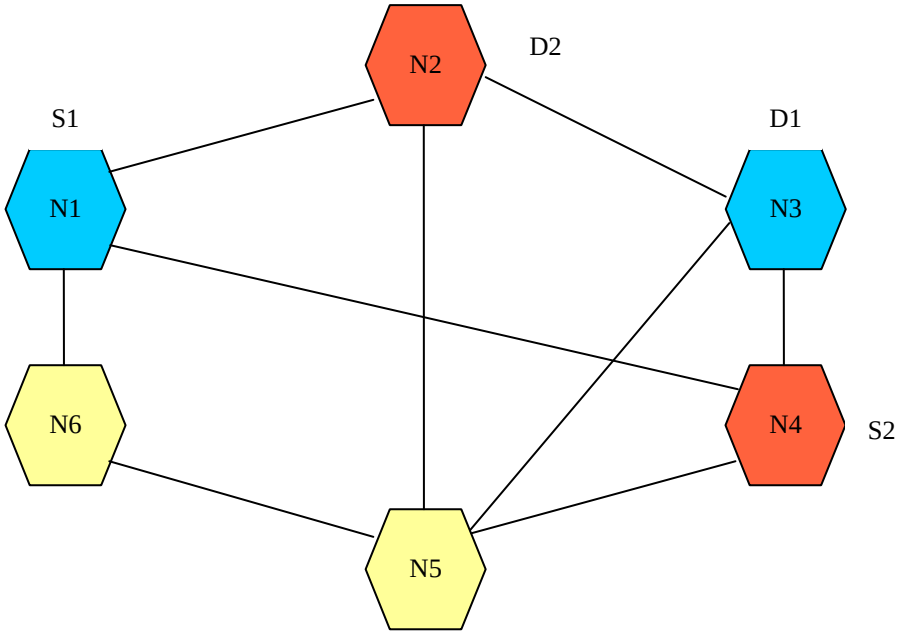
Şekil 3.6 Düğüm hatası ya da ağdan düğüm çıkarılması



Şekil 3.7 Ağa düğüm eklenmesi

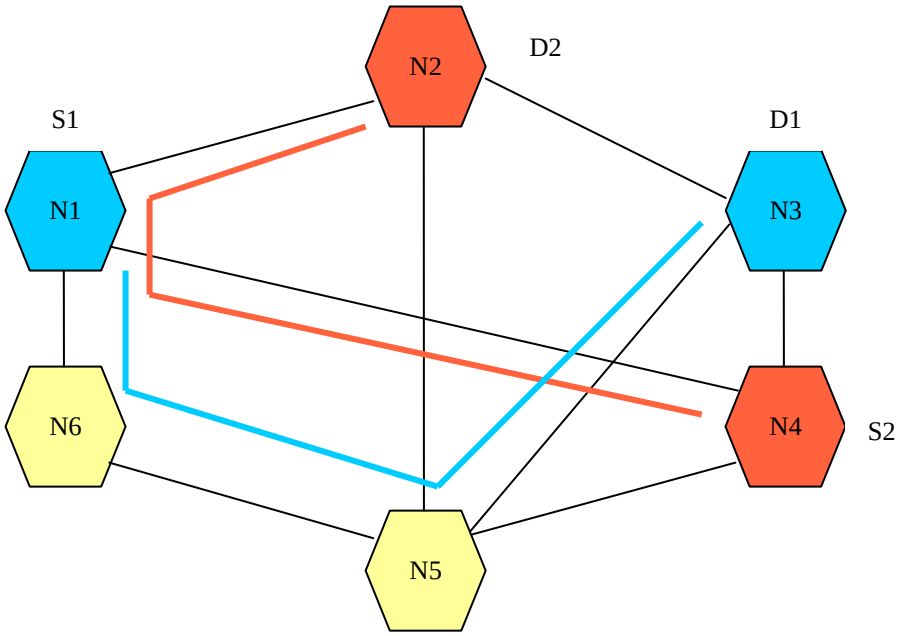
3.4.2 Hata Bağışıklığı Yönetici Protokolü İçin Örnek Çalışma

Aşağıdaki şekillerde bir hata senaryosu için, önerilen protokolün çalışma şekli gösterilmiştir. Başlangıç durumunda fiziksel topoloji (G) ve trafik matrisi ($S=\{N_1,N_4\}$ ve $D=\{N_2,N_3\}$ kümeleri) bilinmektedir. Her bir fiberde kullanılabilecek dalgaboyu sayısı W = 3 olarak verilmiştir.



Şekil 3.8 Fiziksel topoloji, kaynak ve hedef düğümler

Öncelikle, RSVP-TE protokolü kullanılarak istenen veri akışlarını sağlayacak ışıkyolları kurulur (N_1->N_3 ve N_4->N_2) ve bu yollar Işıkyolu Tablosuna kaydedilir.



Şekil 3.9 İstenen trafik matrisi için kurulan ışıkyolları

Tablo 3.3 (a) N_4 düğümü için Işıkyolu Tablosu, (b) N_1 düğümü için Işıkyolu tablosu

Veri Akışı No	Hedef	Yol
1	N_2	N_1N_2

(a)

Veri Akışı No	Hedef	Yol
1	N_3	$N_6N_5\ N_3$

(b)

Bir *t* anında, N_1 ve N_4 arasındaki fiberde bir hata meydana geldiğini düşünelim. Bu durumda;

N_1 düğümü:

- Fiziksel katmanda LoL protokolü ile bu hatayı sezer.
- Yönetici katmana bildirir.
- Yönetici katman, ağ katmanına OSPF tablosunu güncelleme isteğinde bulunur.
- Yönetici katman, Işıkyolu Tablosunu kullanarak, kendi veri akışının etkilenmediğini görür.
- Çözüm için harekete geçmez. Sadece diğer kaynak düğümlere, bu senaryoda N_4, hatayı bildiren bir rapor mesajı gönderir.

Öte yandan N_4 düğümü, hatayı üç farklı şekilde öğrenir:

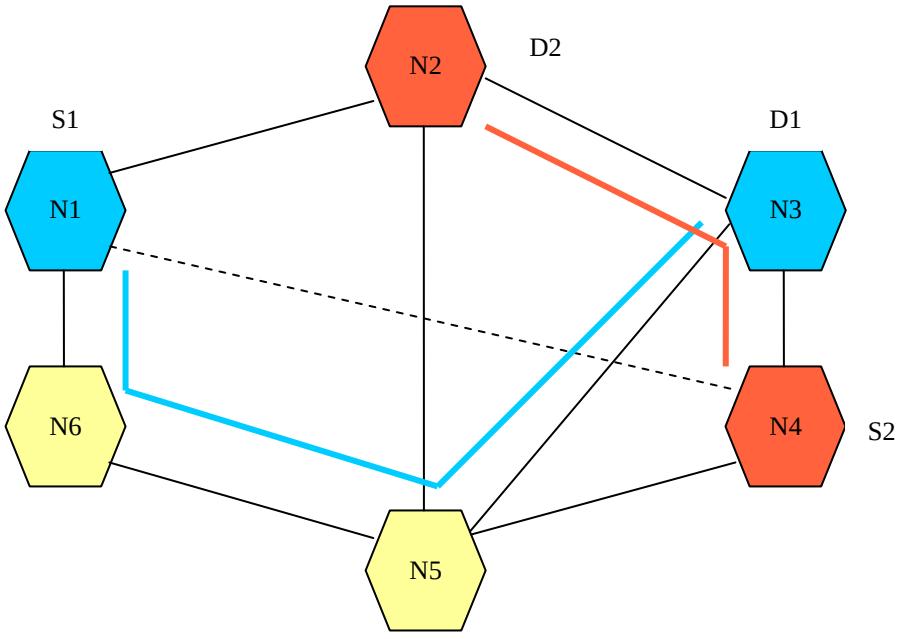
- Fiziksel katmanda LoL protokolü ile
- N_1'den gelen mesajla
- OSPF-TE protokolü aracılığı ile

Normal çalışma şartları altında, bu hatayı yönetici katmana ilk bildiren, fiziksel katmandır. Hata bildirildiğinde yönetici katman:

- Işıkyolu Tablosunu kullanarak hatadan etkilendiğini görür.

- Ağ katmanına OSPF tablosunu güncelleme isteğinde bulunur.
- RSVP-TE aracılığı ile yeni bir ışıkyolu kurar.
- Işıkyolu Tablosunu günceller.

Protokolün çalışma prensibinde, kaynak düğümler bir hata sezdiklerinde öncelikli olarak onarma işlemlerini yürütür, ardından diğer kaynaklara hatayı raporlarlar. Örnek senaryoda, hatadan etkilenen N_4 düğümü, hatayı fiziksel katmanın sezmesiyle onarma işlemlerine başlar. Yeni ışıkyolu kurulduğunda, hata ile ilgili N_1'in rapor mesajı ya da OSPF-TE mesajı N_4'e ulaşmadıysa N_4, diğer kaynak düğümlerin hatadan haberdar olmadıklarını düşünür. Bundan dolayı bir rapor mesajı yollar. Aksi taktirde, tekrar bir raporlama yapmaz. Ayrıca, fiziksel katman tarafından hata sezildikten sonra, N_1'den gelen rapor ve OSPF-TE mesajı daha önce öğrenilmiş bir hatayı bildirdiklerinden dikkate alınmaz. Aşağıdaki şekilde kurulan yeni ışıkyolu ile ağın yeni durumu gösterilmektedir.

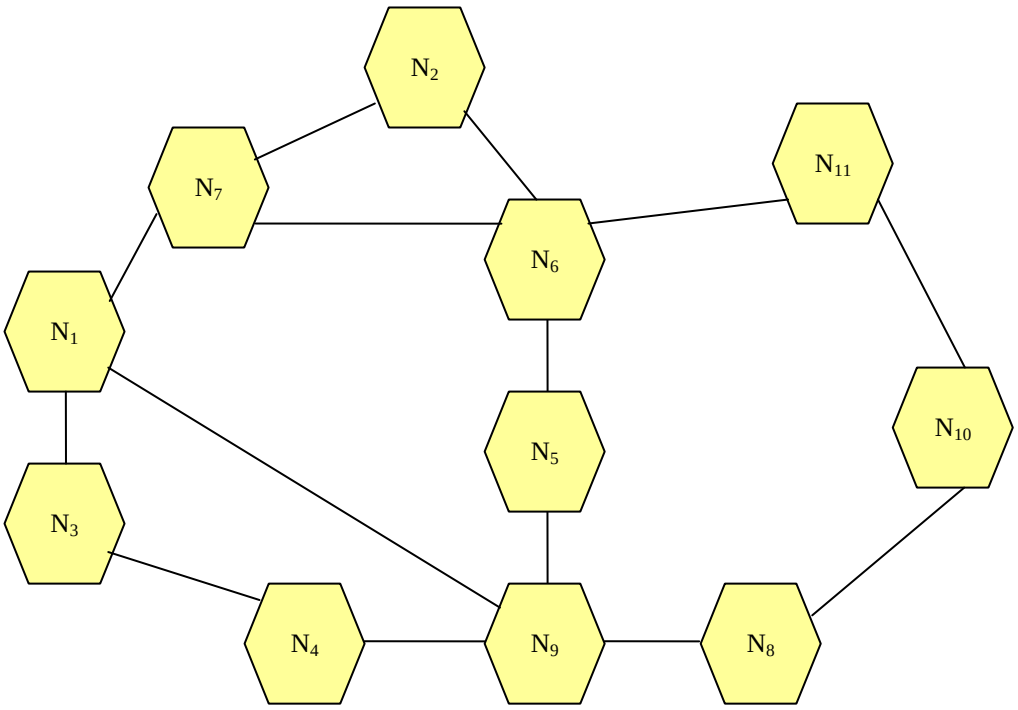


Şekil 3.10 N_1-N_4 arasındaki fiberde oluşan hata sonrası kurulan yeni ışıkyolu

4. BENZETİM PROGRAMI SONUÇLARI

Önerilen protokolün çalışmasını sınamak üzere, C++ kullanılarak, bir benzetim programı gerçeklenmiştir. Bu benzetim programı ile, fiziksel topolojisi ve trafik matrisi bilinen bir ağda hatalar ve topoloji değişiklikleri üretilmiş ve önerilen protokolün davranışı gözlenmiştir. Elde edilen sonuçlar, hatalar sonucu kaybolan veri miktarının ağda taşınan tüm veri miktarına oranı cinsinden verilmiştir.

Testler, Şekil 4.1'de verilmiş olan 11 düğümden oluşan ağ için yapılmıştır.



Şekil 4.1 Testlerde kullanılan ağın fiziksel topolojisi

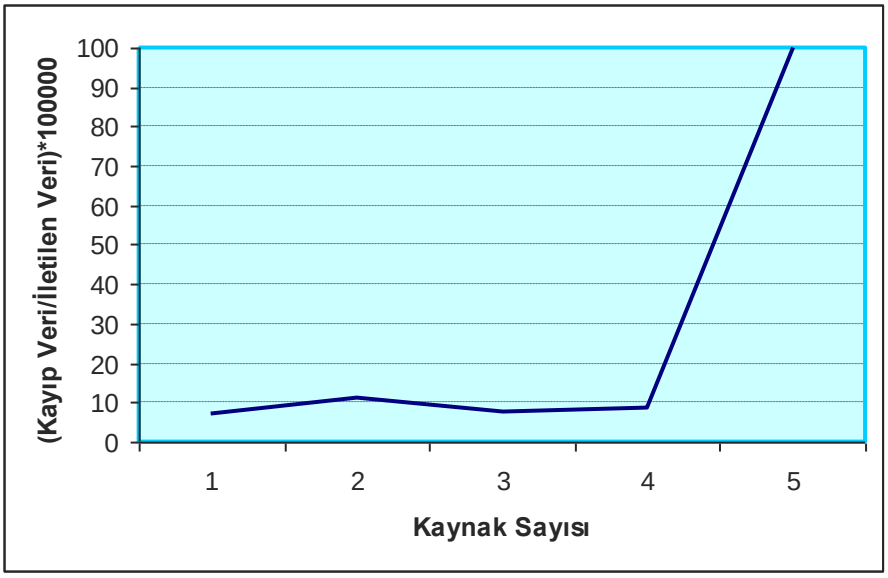
Koşturulan tüm testlerde;

- Bir anda tek bir hata oluşabileceği var sayılmıştır (single failure scenario)
- Her veri akışı, 40 Gb/s hızında kabul edilmiştir
- Hata ya da topoloji değişikliğinin meydana gelme hızı 1 hata/dakika'dır

Belli bir hata sonucu ne kadar veri kaybolduğunu hesaplayabilmek için, hatadan ya da topoloji değişikliğinden etkilenen veri akışlarının yeniden yönlendirilmesi için geçen sürenin bilinmesi gerekmektedir. Bu sürenin hesaplanmasında aşağıdaki değerler kullanılmıştır:

- Doğrudan bağlı düğüm ya da hatlardaki hatanın sezilmesi: 100 µs
- Uzaktaki hataların sezilmesi : 1 ms
- Hatanın etkisinin belirlenmesi : 1 ms
- Tabloların güncellenmsi : 2 ms
- Yeni ışıkyolu kurulması için gerekli herbir adım : 2 ms

Aşağıda yer alan grafikte, ağ üzerinden veri gönderen kaynak sayısındaki artışın veri kaybına etkisi incelenmiştir. Bu senaryoda, her bir hatta kullanılabilecek dalgaboyu sayısı W = 3 olarak kabul edilmiştir.

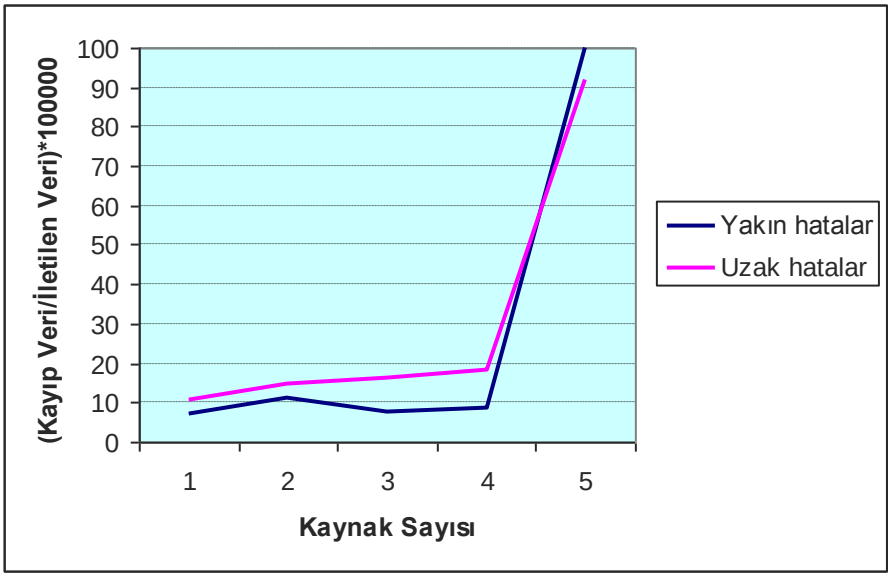


Şekil 4.2 Kaynak sayısının veri kaybına etkisi

Şekil 4.3'te verilmiş olan grafikte, iletim hatlarında kullanılabilecek dalgaboyu (W) sayısının veri kaybına etkisi gösterilmiştir. Bu testlerde, 3 kaynak ve 3 hedeften oluşan sabit bir trafik matrisi kullanılmıştır.

Şekil 4.3 Dalgaboyu sayısının veri kaybına etkisi

Şekil 4.4'te yer alan grafik, hataların kaynaklara olan uzaklığının veri kaybına etkisini göstermektedir. Grafikten de görülebileceği gibi, kaynaklara doğrudan bağlı olan fiber hatlar ya da düğümlerde meydana gelen hatalar daha hızlı sezildiğinden, bunlardan kaynaklanan veri kaybı uzaktaki hatalara göre daha az olmaktadır.



Şekil 4.4 Hata uzaklığının veri kaybına etkisi

5. SONUÇ

Bu tez çalışmasında, optik WDM ağlarında hata bağışıklığı sağlamak üzere bir yönetici protokol geliştirilmiştir. Önerilen protokolle WDM ağlarında hataların daha hızlı sezilmesi ve daha hızlı onarılması; dolayısıyla veri kaybının en aza indirilmesi amaçlanmıştır.

Bu amaç doğrultusunda, öncelikle halen kullanılmakta veya geliştirilmekte olan hata bağışıklığı yöntemleri incelenmiş ve bunların önerilen protokolde nasıl kullanılacağına karar verilmiştir. Dinamik yapısı ve kaynakları daha etkin kullanmasından dolayı onarma yöntemi benimsenmiştir.

Protokolün tasarlanmasında dikey bir hiyerarşi yerine, ulaşım katmanından fiziksel katmana kadar olan katmanları kapsayan bir yapılanma tercih edilmiştir. Böylece, yönetici katmanın diğer katmanlarla doğrudan haberleşebilmesi sağlanmış ve bu da hataların sezilmesini çabuklaştırmıştır.

Protokolün tasarlanmasından önce, yapıyı sınırlayan birtakım varsayımlar yapılmıştır. Bunlardan en önemlisi, trafik matrisinin sabit kabul edilmesidir. Veri kaynaklarının çok az değiştiği omurga ağlarda bu sınırlamanın etkisi önemsizdir. Bununla birlikte, hata bağışıklığı yönetici protokolünün daha geniş bir uygulama alanı bulabilmesi için bu kısıt ortadan kaldırılmalıdır.

Protokolün en önemli hedefi hataları hızla sezmek ve tepki göstermektedir. Bunun için, Bölüm 3'te anlatılan çeşitli optimizasyonlar yapılmıştır. Şekil 4.4'te de gösterildiği gibi, hatalar ne kadar hızlı sezilirse, ağda taşınan veride meydana gelen kayıpların oranı da o kadar az olmaktadır. Sonuç olarak, protokol beklenen verimlilikte çalışma bakımından eksiklere sahip olmakla birlikte, ulaşmak için yola çıktığı hedefe yaklaşmış bulunmaktadır.

KAYNAKLAR

[1] **Maier G., Pattavina A., De Patre S., and Martinelli M.,** 2002. Optical Network Survivability: Protection Techniques in the WDM Layer, *Photonic Network Communications*, **4:3/4**, 251-269.

[2] **Ho P. H. and Mouftah H. T.,** 2004. Shared Protection in Mesh WDM Networks, *IEEE Communications Magazine,* 70-77

[3] **Alanqar, W. and Jukan, A.,** 2004. Extending End-to-End Optical Service Provisioning and Restoration in Carrier Networks: Opportunities, Issues, and Challenges, *IEEE Communications Magazine*, 52-60

[4] **Sahasrabuddhe, L., Ramamurthy A., and Mukherjee B.,** 2002. Fault Management in IP-Over-WDM Networks: WDM Protection Versus IP Restoration, *IEEE Journal on Selected Areas in Commınications,* **20,** 21-33.

[5] **Colle, D., Maesschalck, S., Develder, C., Heuven, P., Groebbens, A., Cheyns, I. L., Pickavet, M., Lagasse, P., and Demeester, P.** 2002. Data-Centric Optical Networks and Their Survivability, *IEEE Journal on Selected Areas in Commınications,* **20,** 6-20.

[6] The International Engineering Consortium, Web ProForum Tutorials, web sayfası: http://www.iec.org

[7] RFC-3209, 2001. RSVP-TE: Extensions to RSVP for LSP Tunnels, *The Internet Society*

[8] **RFC-3473,** 2003. Generalized Multi-Protocol Label Switching (GMPLS) Signalling Resource Reservation Protocol – Traffic Engineering (RSVP-TE) Extensions, *Internet Engineering Task Force (IETF)*

[9] **Sanso, B., Girard, A., and Awad, C.,** A Comparison Between Differentiated Optical Protection and Differentiated Services Protection.

[10] **Maach, A., Bochmann, G. V., and Mouftah, H.,** Shared Protection for Time Slotted Optical Networks, *School of Information Technology & Engineering University of Ottawa*, Canada.

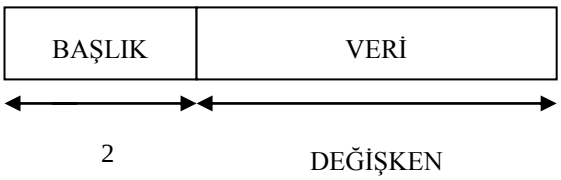
[11] **RFC-793,** 1981. Transmission Control Protocol, *Information Sciences Institute University of Southern California*, California.

[12] **Li, G., Yates, J., Wang, D., and Kalmanek, C.,** Contorl Plane Design for Reliable Optical Networks, *AT&T Labs-Research*

[13] **Vinodkrishnan, K., Durresi, A., Chandhuk, N., Jain, R., Jagannathan, R., and Seetharaman, S.,** Survivability in IP Over WDM Networks, *Department of Computer and Information Science,* The Ohio State University.

EK A. HATA BAĞIŞIKLIĞI YÖNETİCİ PROTOKOLÜ MESAJ YAPISI

Temel mesaj yapısı:



Alt katmanlardan yönetici protokole giden bildirim mesajları:

Yerel cihazda hata	Veri içermez
Komşu cihazda hata	Düğüm_numarası
Doğrudan bağlı fiberde hata	Fiber_numarası
Yeni fiber ekleme	Fiber_numarası Bağlantı_bilgileri
Yeni düğüm ekleme	Düğüm_numarası Bağlantı_bilgileri
Ağdan düğüm çıkarma	Düğüm_numarası
Ulaşım katmanı hatası	Hata_bilgileri

Yönetici katmandan alt katmanlara giden istek mesajları:

OSPF tablosuna ekleme	Düğüm_fiber_bilgisi Numarası Bağlantı_bilgileri

OSPF tablosundan silme	Düğüm_fiber_bilgisi Numarası

Yeni ışıkyolu kur	Kaynak_düğüm_numarası Hedef_düğüm_numarası

ÖZGEÇMİŞ

Hülya Hocaoğlu, 18 Ağustos 1980 tarihinde Bulgaristan'ın Eski Cuma şehrinde dünyaya geldi. İstanbul Teknik Üniversitesi Bilgisayar Mühendisliği Bölümü'nde 1999 yılında başladığı lisans eğitimini 2003 yılında tamamlayarak Bilgisayar Mühendisi ünvanını aldı. 2003-2004 öğretim yılında Kadir Has Üniversitesi Mühendislik Fakültesi'nde araştırma görevlisi olarak görev yaptı. Halen Nortel NETAŞ'ta AR-GE mühendisi olarak çalışmaktadır.