



## **402 BİLGİSAYAR AĞLARI DERSİ**

### **ARAŞTIRMA ÖDEVİ-II**

Ayben GÜLNAR-191180041

**MART 2023**

## İçindekiler Tablosu

Şekiller Listesi .....	2
1.GİRİŞ .....	3
2. PAKET ANAHTARLAMALI AĞLARIN TEMEL YAPILARI VE KUYRUK YÖNETİMİ KAVRAMLARI.....	3
2.1 Paket Anahtarlama Tanımı, Avantaj & Dezavantajları .....	3
2.2. Sonsuz Depolamalı Paket Anahtarları (Packet Switches with Infinite Storage) .....	4
2.3 Fairness In Packet-Switching Systems .....	5
3.YÜKSEK HIZLI PAKET ANAHTARLARI İÇİN ÖLÇEKLENEBİLİR DONANIM ÖNCELİK SIRALI KUYRUK MİMARİLERİ .....	7
4.KUYRUK YÖNETİMİ PERFORMANSININ ÖLÇÜMÜ VE DEĞERLENDİRİLMESİ....	9
5.BÜYÜK ÖLÇEKLİ PAKET ANAHTARLAMALI AĞLARDA KUYRUK YÖNETİMİ ZORLUKLARI VE ÇÖZÜMLERİ.....	11
6.KUYRUK YÖNETİMİ İLE İLGİLİ GELECEKTEKİ ARAŞTIRMA VE GELİŞTİRME ALANLARI .....	12
7.SONUÇ .....	14
8.KAYNAKÇA.....	15

## Şekiller Listesi

Şekil 2.1.1 Paket Anahtarlama .....	4
Şekil 2.2.1 First in First out queue .....	5
Şekil 2.3.1 Fair Queue .....	6
Şekil 3.1 .....	8
Şekil 3.2 .....	9
Şekil 4.1 .....	10

## 1.GİRİŞ

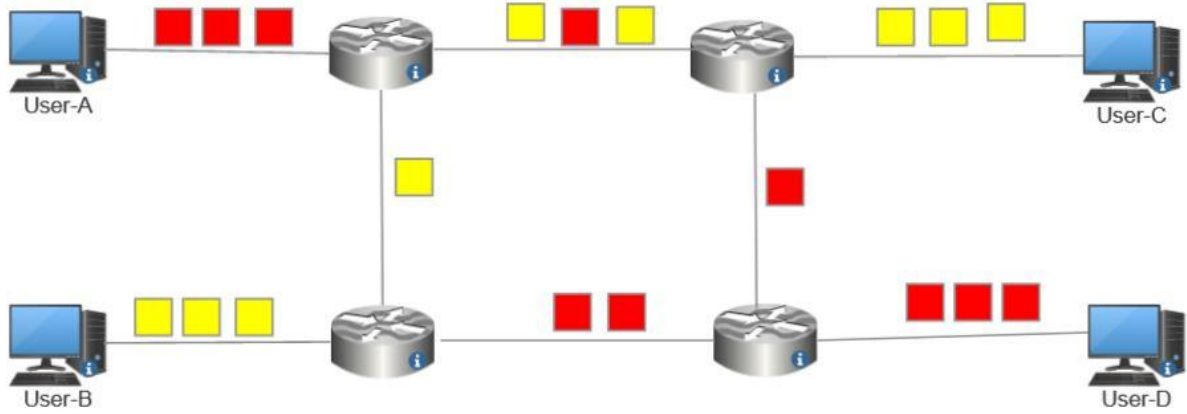
Son yıllarda, veri iletişimi, paket anahtarlama olarak adlandırılan hızla yeni bir teknoloji ile devrim geçirmiştir. 1968'de neredeyse tüm etkileşimli veri iletişim ağları, telefon ağıyla aynı şekilde devre anahtarlama idi. Devre anahtarlama ağlar, bir çağrı veya oturum için iletim bant genişliği tahsis eder. Ancak, etkileşimli veri iletişimi kısa patlamalar halinde gerçekleştiğinden, bant genişliğinin %90'ı veya daha fazlası israf edilir. Bu nedenle, dijital elektronik yeterince ucuz hale geldikçe, iletişim ağlarının tamamen değiştirilmesi, iletim bant genişliğinin dinamik olarak tahsis edilmesine izin veren paket anahtarlama kavramını tanıttı ve daha önce bir kullanıcı için gereken iletim hattını birçok kullanıcının paylaşmasına izin verdi. Paket anahtarlama, veri iletişiminin ekonomisini geliştirmekle kalmayıp, güvenilirliği ve işlevsel esnekliği de artırdığı için, dünya genelinde 1978'de yapılan neredeyse tüm yeni veri ağları, paket anahtarlama dayandırılmaktadır. Son zamanlarda ortaya çıkan uygulamaların çeşitli kalite-of-servis gereksinimlerini karşılamak için etkili paket zamanlama mekanizmalarına sahip modern entegre ağlar kullanılmaktadır. Ancak yüksek hızlı bir bağlantıda çok sayıda küçük paket arasında ayırım yapmak, öncelikli bir kuyruğun verimli bir donanım uygulamasını gerektirir [1].

Bu ödevimde, paket anahtarlama ağların ne olduğu ve bu ağlarda kuyruk yönetimi incelenmiş olup ikisi arasındaki ilişki detaylıca ele alınmıştır.

## 2. PAKET ANAHTARLAMALI AĞLARIN TEMEL YAPILARI VE KUYRUK YÖNETİMİ KAVRAMLARI

### 2.1 Paket Anahtarlama Tanımı, Avantaj & Dezavantajları

Paket anahtarlama kullanıcılar, verilerini göndermeden önce daha küçük paketlere bölerler. Her paketin bir paket başlığı vardır ve bu başlık, paketin türü, kaynak adresi, hedef adresi ve mesaj içindeki paket sırası gibi bilgileri içerir. İnternet, bir paket anahtarlama ağ örneğidir. Bu tür bir ağda, düğümler terminal ve ana bilgisayarlar arasında bilgi alışverişi yapmak zorundadır. Bu paket anahtarlama sisteminin genel işlevi, terminaller ve ana bilgisayarlar arasında verinin şeffaf bir şekilde küçük paketler halinde değiş tokuş edilmesidir. Terminaller ve ana bilgisayarlar paketleri yönlendirmek yerine sadece hedefi belirtirler.



Şekil 2.1.1 Paket Anahtarlama

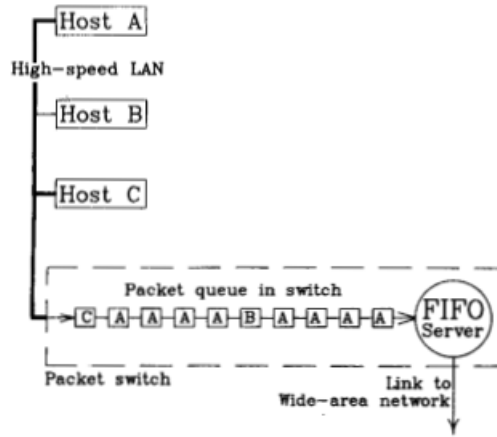
Paketler, hedef adresini taşıdığından dolayı ağ üzerinden ayrı ayrı yönlendirilebilirler. Uyarlamalı yönlendirmede, gecikmeyi en aza indirecek rotayı izlerler. Her paket hedef adresini içerdiği için, aynı mesajdaki paketler tamamen farklı rotalardan geçebilir ve yine de aynı hedef adresine ulaşabilirler. Örneğin: Yukarıdaki şekilde, kullanıcı-A kırmızı paketleri kullanıcı-D'ye, kullanıcı-B ise sarı paketleri kullanıcı-C'ye gönderir. Aynı kullanıcı ve mesajdaki paketlerin farklı yollar izleyebileceğini görüyoruz. Aradaki düğümler (yönlendiriciler) paketleri hedefe ulaşana kadar iletmeye devam ederler. Paket anahtarlama ağlarında, kullanıcılar birbirleriyle dolaylı olarak iletişim kurarlar. Bu, uçtan uca iletişim olmadığı anlamına gelir. Dolayısıyla, bu anahtarlama türü, paketlerin hızlı bir şekilde hedefe yönlendirilmesi nedeniyle daha az bant genişliği kullanır. Paket anahtarlama, büyük bir alan kaplamaz. Bir paket kaybı durumunda, mesajı tamamlamak için bir kopya isteyebiliriz. Paket anahtarlama iletişimi gecikme kabul etmeyen uygulamalar için uygun değildir. Sesli aramalar bu duruma örnektir. Yüksek kurulum maliyeti vardır [2].

## 2.2. Sonsuz Depolamalı Paket Anahtarları (Packet Switches with Infinite Storage)

İsterseniz sonsuz depolama kapasitesine sahip basit bir paket anahtarından bahsederek başlayalım. Bir anahtarın giriş ve çıkış bağlantıları vardır. Her bağlantı sabit bir veri aktarım hızına sahiptir. Tüm bağlantıların aynı veri hızına sahip olması gerekli değildir. Paketler giriş bağlantıları üzerinden gelir ve burada incelenmeyen bir yönlendirme mekanizması tarafından hemen bir çıkış bağlantısına atanır. Her çıkış bağlantısı bir kuyruğa sahiptir. Paketler bu kuyruktan çıkarılır ve çıkış bağlantısına, o bağlantının veri hızına uygun şekilde gönderilir. İlk olarak, kuyrukların first-in, first-out şekilde yönetildiğini varsayacağız. Paketlerin bir son kullanma tarihi vardır. DoD IP protokolünde, paketlerin ilgi çekici olmayan olarak atılması gereken süre olan bir time-to-live alanı bulunur. Paket ağ boyunca seyahat ederken, bu alan azaltılır; sıfır olursa paket atılmalıdır. Bu alanın başlangıç değeri sabittir; DoD IP protokolünde, bu değer varsayılan olarak 15'tir. Time-to-live mekanizması, kuyrukların sınırsız bir

şekilde büyümesini önler; kuyruklar yeterince uzun hale geldiğinde, gönderilmeden önce paketler zaman aşımına uğrayacaktır. Bu, tüm kuyrukların toplam boyutu için bir üst sınır belirler; bu sınır, tüm gelen bağlantıların veri hızı ve zaman aşımının üst sınırı tarafından belirlenir.

Ancak, bu tıkanıklığı ortadan kaldırmaz. Nedenine bakalım. Basit bir düğümü ele alalım, tek bir gelen bağlantı ve tek bir çıkan bağlantısı olan, Şekil 2.2.1'de gösterildiği gibi. Düğüme birçok ana bilgisayar paketi üretebilir ve gelen bant genişliği, çıkan bant genişliğinden daha fazladır. Şekilde, kaynak ana bilgisayarını ve her paketin zaman aşımı değerini gösteriyoruz. Ana bilgisayar A, trafiğin büyük bir kısmını oluşturuyor ve çıktı bağlantısını tek başına doyuracak kadar trafik üretiyor. Paketler önce ilk gelen ilk çıkar şeklinde kuyruklanır ve tüm ana bilgisayarlar aynı başlangıç zaman aşımı değerini kullanır. Paketler bu nedenle zaman aşımına göre azalan sırayla sıralanır.



Şekil 2.2.1 First in First out queue

Bir düğümde paket varış hızı, çıkış hızından fazla olduğunda, çıkan bağlantının kuyruk uzunluğu zaman aşımı değeri olan gelen paketlerin transit süresini aştığı noktaya kadar artar. Bu noktada, çıktı bağlantısını işleyen işlem, kuyruktan paketleri çıkarırken bazen zaman aşımı alanı sıfıra indirilmiş bir paket bulacaktır. Böyle bir durumda, o paketi atacak ve sıradaki paketle tekrar deneyecektir. Sıfır zaman aşımı alan paketler gönderilemeyecektir.

Gönderilen paketlerin zaman aşımı alanları sıfır olmayacaktır. Ancak, aşırı yük altında istikrarlı durum elde edildikten sonra, bu değerler küçük olacaktır çünkü paket en fazla zaman aşımı değerinin hafifçe altında kuyrukta kalmış olacaktır. Aslında, çıkış hızı, her zaman bir zaman aşımı birimi başına birinden büyük olduğunda, iletilen herhangi bir paketin zaman aşımı değeri tam olarak bir olacaktır [3].

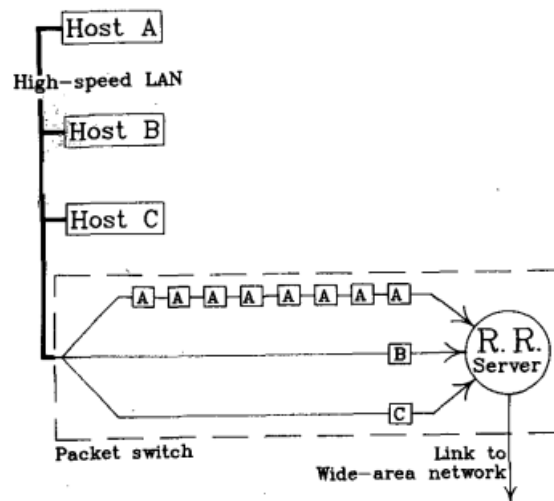
### 2.3 Fairness In Packet-Switching Systems

Hızlı-datagram yerel ağlarının (Ethernet ve çoğu IEEE 802.x datagram sistemleri, taşıyıcı algılama veya simge geçişine dayansınlar, olsunlar) ve bu yerel ağlara bağlı ana bilgisayarların ve paket anahtarları ve uzun mesafeli bağlantılardan oluşan birbirine bağlı geniş alan ağından

oluşan bir ağı ele alalım. Geniş alan ağı dahili akış kontrolüne sahip olabilir, ancak kaynak ana bilgisayarlara zorunlu akış kontrolü uygulama yolu yoktur. DoD Internet, Xerox Network Systems internet ağları ve bunlardan türetilen ağlar bu modele uyar.

Yerel ağıdaki herhangi bir ana bilgisayar, geniş alan ağı tarafından absorbe edebileceğinden daha hızlı bir hızda yönlendirilen paketler oluştursa, yerel ve geniş alan ağlarını birbirine bağlayan paket anahtarı üzerinde tıkanıklık oluşur. Eğer paket anahtarları sadece ilk gelen ilk çıkar (FIFO) prensibine göre kuyruk yaparlarsa, kötü davranışlı ana bilgisayar diğer daha iyi davranışlı ana bilgisayarların veri iletimine müdahale edecektir.

Adil olma kavramını tanıtıyoruz. Paket anahtarlarımızı adil hale getirmek istiyoruz, yani her kaynak ana bilgisayar her paket anahtarının eşit bir bölümünü elde edebilmelidir. Bu, her çıkan bağlantı için ilişkilendirilmiş tek bir FIFO kuyruğunu her kaynak ana bilgisayar için bir kuyruk ile değiştirerek yapabiliriz. Şekil 2'de gösterildiği gibi. Şekil 1 için geçerli olan kurallar burada da geçerlidir, ancak bu kez kuyrukları sırayla döndürerek hizmet ediyoruz. Sırayla boş olmayan her kuyruktan bir paket alınır ve ilgili çıkan bağlantıdaki zaman aşımı değeri pozitif olan paketler iletilirken süresi dolan paketler bırakılır. Boş kuyruklar atlanır ve sıra kaybederler. Kuyruklar hedef ana bilgisayar yerine kaynak ana bilgisayara göre belirlenir, çünkü paket üretimini kontrol eden kaynakları adil olmaya çalışır.



Şekil 2.3.1 Fair Queue

Bu mekanizma adil bir şekilde çalışır; çıkış bağlantısı bant genişliği, kaynak ana bilgisayarlar arasında eşit olarak bölünür. Belirtilen çıkış bağlantısı için anahtarlanmış paketi olan her kaynak ana bilgisayar, round-robin algoritması döndüğünde çıkış bağlantısında tam olarak bir paket gönderir. Böylece bir yük dengelemesi şekli uygulanmış olduk.

Belirli bir ana bilgisayar için en uygun strateji artık mümkün olduğunca çok paket göndermek değildir. En uygun strateji, her paket anahtarında tam olarak bir paket bekleyecek şekilde paket gönderme hızını ayarlamaktır, böylece round-robin algoritması döndüğünde ana bilgisayarın servis edilmesi sağlanacak ve paketlerin minimum geçiş gecikmesi olacaktır. Bu strateji genel olarak her kuyruğun uzunluğunun 1 ile 2 arasında olacağından ağın görünümü açısından oldukça kabul edilebilir.

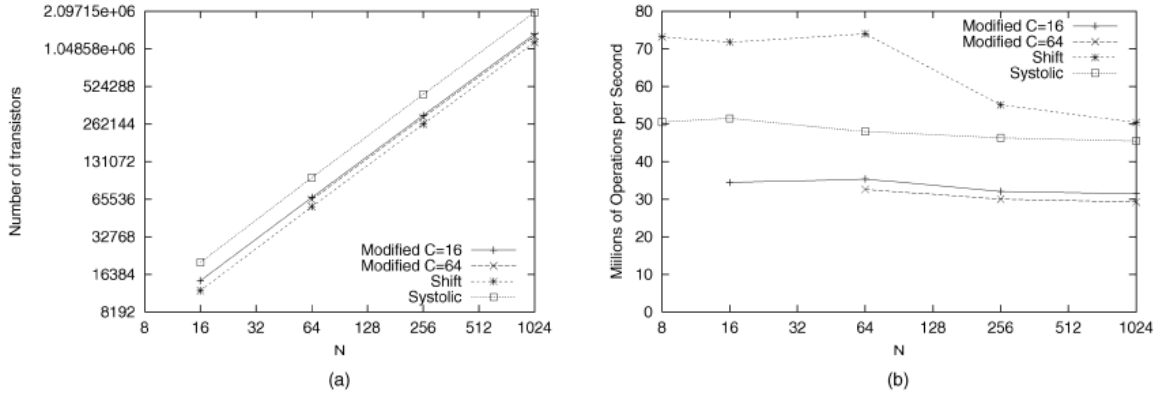
Ana bilgisayarlar, stratejilerini optimize etmek için ağdan tavsiye bilgisiyle ihtiyaç duyarlar. DoD IP'deki mevcut Kaynak Sıkışıklığı mekanizması, minimal olsa da bunu sağlamak için yeterlidir. Anahtarlanmış paketlerin sayısı küçük bir değeri (muhtemelen 2) aştığında, paket anahtarları, o kaynak ana bilgisayarına bir Kaynak Sıkışıklığı mesajı göndermelidir. Ana bilgisayarlar, kaynak sıkışıklığı mesajlarını aldıkları noktadan hemen önce trafiğini bu değerin altında tutarsa, her ana bilgisayar için ortalama kuyruk uzunluğunun 2'nin altında çalışması beklenir [3].

### 3.YÜKSEK HIZLI PAKET ANAHTARLARI İÇİN ÖLÇEKLENEBİLİR DONANIM ÖNCELİK SIRALI KUYRUK MİMARİLERİ

Yüksek hızlı anahtarlama cihazlarda bağlantı planlaması için iki yeni donanım öncelikli kuyruk mimarisi önerilen ve değerlendirilen makalede Verilog ve Epoch tasarımları ve simülasyonları temel alarak, mevcut dört mimarinin hem N hem de P'ye göre ölçeklenebilirliğinin sınırlı olduğu gösterilmiş. Küçük N ve P için, dört mevcut mimarinin tümü benzer donanım maliyetleri ve performansına sahipti. Ancak, büyük N ve P'yi desteklemek üzere ölçeklendirildiklerinde, her mimarinin kısıtlamaları daha belirgin hale gelmiştir. Dört mimari arasından, kaydırma kayıt mimarisi ve sistolik dizi mimarisi daha iyi ölçeklenebilirdi. İki mimariyi birleştirerek, modifiye edilmiş sistolik mimarisi, iki mimarinin maruz kaldığı ölçeklenme sorunlarının olumsuz etkilerini azalttı. Özellikle, toplam geçici depolama kayıtlarının sayısını azaltarak donanım maliyetleri önemli ölçüde azaltıldı; kaydırma kaydındaki veri yüklenmesi sorunundan kaynaklanan performans kaybı, c uzunluğunda birkaç kaydırma kaydı kuyruğu kullanılarak N'den izole edilip kontrol edilebilir hale getirildi. Burada, c donanım ve performans gereksinimlerini dikkate alarak seçildi. Çoklu sistolik mimarisi, ölçeklenebilirliğe ödün vermeden modifiye edilmiş sistolik mimarisine çoklu bağlantı desteği ekledi. Dequeue ve Enqueue işlemlerine ekstra döngüler eklenmesine rağmen, her iki işlem de, mimari tarafından desteklenen çıkış bağlantılarının sayısı olan N veya M'den bağımsız olarak sabit bir zamanda (döngüde) yapılabilirdi. Ayrıca, M'ye göre ölçeklenmenin çok az ek donanım



eklenerek mümkün olduğunu gözlemledik. Verilog ve Epoch simülasyonları, yeni mimarilerin belirgin özelliklerini onayladı. İki yeni donanım öncelikli kuyruk mimarisinin, N ve P arttıkça iyi ölçeklendiğini gösterdik. Her ikisi de iyi performans sunar ve uygulaması kolaydır, bu nedenle yüksek hızlı ağlarda QoS gereksinimlerinin garanti edilmesinde kullanılabilirler. Bu etkili öncelikli kuyruk uygulamaları, daha agresif bağlantı programlama algoritmalarının kullanılmasına olanak tanır ve çeşitli trafik desenleri ve QoS gereksinimleri olan daha fazla bağlantıyı kabul edebilir. Bu alandaki olası bir gelecekteki araştırma, çeşitli bağlantı programlama algoritmalarının uygulanması ve donanım öncelikli kuyruğun uygulama karmaşıklığını ve performansını karşılaştırmak olabilir. Ayrıca, tüm öncelikli kuyruk mimarilerinin ortak bir arabirimi olduğundan, bu öncelikli kuyrukların öncelik kuyruğu gerektiren diğer uygulamalarda kullanılması kolaylaşır [8].



Şekil 3.1

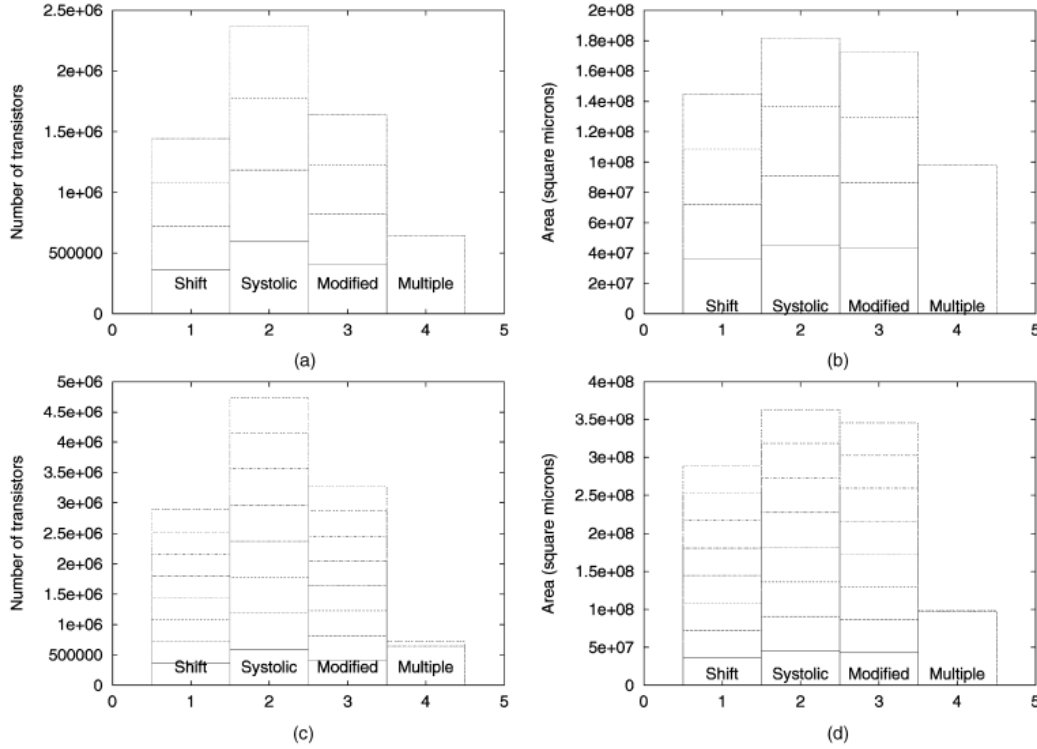


Fig. 19. Implementation comparison with multiple systolic architecture ( $P = 256$ ). (a)  $N = 256$ ,  $M = 4$ . (b)  $N = 256$ ,  $M = 4$ . (c)  $N = 256$ ,  $M = 8$ . (d)  $N = 256$ ,  $M = 8$ .

Şekil 3.2

## 4.KUYRUK YÖNETİMİ PERFORMANSININ ÖLÇÜMÜ VE DEĞERLENDİRİLMESİ

Bilgisayar ağlarında kuyruk yönetimi performansının ölçümü ve değerlendirmesi, ağ trafiğinde meydana gelen kuyruk oluşumunun etkilerinin incelenmesi ve kuyruk yönetim algoritmalarının performansının ölçülmesi için yapılan çalışmalardır. Kuyruk yönetimi, ağdaki paketlerin belirli bir sıraya göre işlem görmelerini sağlayan ve ağ trafiği yoğunluğunu düzenleyen bir yöntemdir. Bu çalışmalar, ağ performansını iyileştirmek ve ağ trafiği yönetiminde kullanılan kuyruk yönetimi algoritmalarının etkinliğini artırmak için önemlidir. Bu kapsamda, ağ trafiğindeki kuyruk oluşumu, kuyruk yönetimi algoritmalarının performansı, paket gecikmesi ve kaybı gibi çeşitli ölçütlere göre değerlendirilir.

İncelediğim makalede: Şekil 1'de gösterilen tek aşamalı  $N \times N$  paket anahtarını ele alalım. Giriş/çıkış bağlantı noktalarının sayısı  $N$ , büyük kabul edilir ( $N \gg 1$ ). Önceki çalışmalar, uzay bölme paket anahtarlarının performansının boyutlarına bağlı olduğunu göstermiştir. Ancak, boyut  $16 \times 16$ 'dan büyüdükçe maksimum verimlilik ve ortalama gecikme arasındaki fark ihmal edilebilir hale gelir. Ayrıca, giriş sıralarındaki kuyruk uzunluğu da dahil olmak üzere diğer ilgi çeken miktarlar için fark da ihmal edilebilir hale gelir. Bu, Zürih Araştırma Laboratuvarı'nda

geliştirilen anahtarın prototipi üzerinde elde edilen deneyimsel sonuçlar ve simülasyon yoluyla doğrulanmıştır. Bu nedenle, burada sunulan sonuçlar 16 veya daha fazla giriş/çıkışa sahip anahtarların performansının çok iyi bir yaklaşımı olarak kabul edilebilir.

Paketlerin sabit bir uzunluğu ve sabit bir iletim süresi  $h$ 'ye sahip olduğu varsayılır. Bundan böyle, bu iletim süresi  $h$ , bir zaman birimi olarak seçilir. Ayrıca, trafiğin simetrik ve rastgele dağıldığı varsayılır. Bu, herhangi bir paketin hedefinin eşit olasılıkla  $N$  çıkış bağlantı noktasından biri olabileceği anlamına gelir.

Çıkış kuyrukları, belirli bir dereceye kadar çıkış bağlantı noktası çekişmelerini çözmek için sağlanmıştır. Her çıkış kuyruğunun birinci gelen ilk hizmet (FIFO) esasına göre çalıştığı ve en fazla  $b$  paketi tutma kapasitesine sahip olduğu varsayılır. Giriş tarafında, bir paket bir giriş kuyruğunun başına geldiğinde, hedef bağlantı noktasına transfer işlemi başlatılır. Çıkış bağlantı noktası boşsa, paket kesintisiz bir şekilde anahtarın içinden akar ve herhangi bir gecikme yaşamaz. Ancak, çıkış bağlantı noktası meşgulse ve bu bağlantı noktasına ait çıkış önbellegi dolu değilse, paket transfer edilir ve burada saklanır. Ancak, önbelleg doluyorsa geri basınç sinyali uygulanır ve paket giriş kuyruğunun başında beklemek zorunda kalır. Bu anda, aynı özel çıkış önbellegine gönderilmek üzere bekleyen diğer paketler de olabilir.

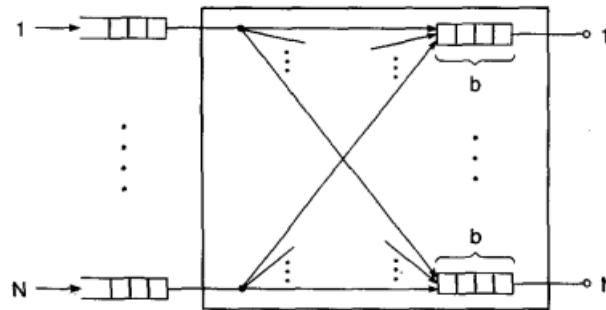


Fig. 1. An  $N \times N$  packet switch with input and output queueing.

#### Şekil 4.1

İncelediğim makalede, geri basınç etkisinin anahtar teslimi anahtarlama cihazının performansına etkisini analiz etmektir. Bu etkinin, çıkış tamponlarının boyutu  $b$ 'ye bağlı olduğu gösterilmiştir. İki farklı anahtarlama modeli ele alınmaktadır. İlk olarak, paketlerin varışı ve çıkış bağlantı noktalarına iletilmesi asenkron bir şekilde gerçekleştiği bir asenkron model ele alınmaktadır. Varış süreci Poisson dağılımına tabi tutulmaktadır. Daha sonra, Bernoulli'ye tabi olarak paketlerin senkron bir şekilde varışı ve iletimi yapılan senkron bir model ele alınmaktadır.

Analitik yaklaşımımız, saf giriş kuyruklu anahtarlama anahtarının analizi için tarafından kullanılan yöntemi izler. Anahtarlama ile ilgili verimlilik, ortalama gecikme ve anahtarlama maksimum verimle kullanabilme kapasitesi ölçüleri temel alınarak değerlendirilir. Paket gecikmesi, üç bileşenden oluşur:

1. Kuyruklarda kafa sırasına gelene kadar bekleyiş süresi,
2. Baş sırası yarışması nedeniyle giriş kuyruklarında bekleyiş süresi,
3. Çıkış bağlantı noktalarında çıkış bağlantı noktası yarışması nedeniyle bekleyiş süresi.

İkinci ve üçüncü gecikme bileşenleri, eşdeğer tek sunuculu kuyruk sistemlerinin özel bir çalışması temel alınarak açıkça hesaplanmaktadır. Daha sonra, ilk gecikme bileşeni, önceki çalışmanın sağladığı hizmet özelliklerinin bir başka tek sunuculu kuyruk sistemi tarafından sağlandığı şekilde elde edilir. Analiz, hem asenkron hem de senkron model için yapılmaktadır [4].

## 5.BÜYÜK ÖLÇEKLİ PAKET ANAHTARLAMALI AĞLARDA KUYRUK YÖNETİMİ ZORLUKLARI VE ÇÖZÜMLERİ

Bu başlık, büyük ölçekli paket anahtarlama ağılarda kuyruk yönetimi zorlukları ve bu zorlukların çözümüne yönelik araştırmaları ifade etmektedir. Büyük ölçekli ağlar, milyarlarca cihaz ve kullanıcının birbirine bağlandığı karmaşık ağ yapısıdır ve bu ağlarda paketlerin yönetimi, yönlendirilmesi ve teslim edilmesi ciddi zorluklar doğurabilir. Bu nedenle, kuyruk yönetimi gibi ağ trafiğinin yönetimini sağlayan tekniklerin performansı, ağın genel performansı açısından kritik bir öneme sahiptir. Bu başlık altında incelenen konular arasında, kuyruk yönetimi algoritmalarının özellikleri, farklı kuyruk yönetimi yöntemlerinin avantajları ve dezavantajları, kuyruk yönetimi performansının ölçümü ve analizi, sıralama ve önceliklendirme teknikleri, kuyruk boyutu kontrolü, hizmet kalitesi garantisi (QoS) sağlama ve güvenilirlik konuları yer alabilir. Büyük ölçekli paket anahtarlama ağılar, yüksek hızlı iletişim ve büyük bant genişliği gereksinimleri nedeniyle önem kazanmıştır. Ancak, bu ağlardaki yüksek veri trafiği, kuyruk yönetimi problemlerini ortaya çıkarır. Bu problemler arasında kuyruklar arasındaki adil paylaşım, ağın doğru şekilde ölçeklendirilememesi, kuyruk boyutu ve paket kaybı önleme gibi konular bulunur.

Bu nedenle, büyük ölçekli ağlarda kuyruk yönetimi performansının ölçülmesi ve değerlendirilmesi büyük önem taşır. Bu ölçüm ve değerlendirme, ağın performansını artırmak için etkili kuyruk yönetimi tekniklerinin geliştirilmesine yardımcı olabilir. Bu teknikler

arasında, kuyruk boyutlarının dinamik olarak ayarlanması, sıralama ve kuyruklar arasında adil paylaşım sağlanması, paketlerin önceliklendirilmesi ve akış kontrolü bulunur.

Kuyruk yönetimi performansının ölçümü ve değerlendirilmesi için çeşitli yöntemler bulunmaktadır. Bunlar arasında, simülasyon, analitik modelleme ve deneysel çalışmalar yer alır. Bu yöntemler, ağın farklı senaryolarda nasıl davrandığını ve performansının hangi faktörlerden etkilendiğini anlamak için kullanılabilir [5].

Araştırdığım bir diğer makaleye göre, büyük ölçekli paket anahtarlama ağılarda kuyruk yönetimi zorluklarını ele almakta ve çözüm önerileri sunmaktadır. Makale, kuyruk yönetimi algoritmaları ve performans ölçütlerine kısa bir giriş yaparak başlamaktadır. Daha sonra, büyük ölçekli ağlardaki kuyruk yönetimi zorluklarına değinmektedir. Bu zorluklar arasında, yüksek trafik hacmi, gecikme, kuyruk doluluk durumları ve ağ topolojisi yer almaktadır. Makale, bu zorlukların üstesinden gelmek için önerilen çözümleri de sunmaktadır. Bunlar arasında, sıralı paketleri işleme, kuyruk yönetimi algoritmalarının ve hızlı anahtarlama teknolojilerinin kullanımı, veri paketlerinin önceliklendirilmesi ve ağ topolojisinin yeniden düzenlenmesi yer almaktadır. Makale, büyük ölçekli ağlarda kuyruk yönetiminin performansını değerlendirmek için kullanılabilecek ölçütleri de ele almaktadır. Bu ölçütler arasında, gecikme süresi, veri kaybı oranı, veri paketleri arasındaki eşitlik ve ağın maksimum bant genişliği gibi faktörler yer almaktadır. Sonuç olarak, makale, büyük ölçekli paket anahtarlama ağılarda kuyruk yönetimi zorluklarının önemini vurgulamakta ve bu zorlukların üstesinden gelmek için önerilen çözümleri sunmaktadır. Ayrıca, ağ performansının ölçülmesi için kullanılabilecek ölçütleri de tartışmaktadır [6].

## 6. KUYRUK YÖNETİMİ İLE İLGİLİ GELECEKTEKİ ARAŞTIRMA VE GELİŞTİRME ALANLARI

Kuyruk yönetimi, ağlarda gelen trafiğin yönetilmesinde önemli bir rol oynamaktadır. Bu nedenle, gelecekteki araştırma ve geliştirme çalışmaları kuyruk yönetimi alanında odaklanabilir. Bunlar, daha verimli ve etkili kuyruk yönetimi teknikleri geliştirmek, daha akıllı kuyruk yönetimi sistemleri tasarlamak ve ağ performansını artırmak için kuyruk yönetimi ile birleştirilebilecek diğer teknolojileri araştırmak gibi konuları kapsayabilir.

Daha verimli kuyruk yönetimi teknikleri, trafiği en iyi şekilde yönetmek için daha akıllı algoritmaların geliştirilmesini içerir. Bunun yanı sıra, kuyruk yönetimi sistemlerinin optimize edilmesi, daha az gecikme, daha yüksek bant genişliği kullanımı ve daha düşük paket kaybı gibi avantajlar sağlayabilir.

Ayrıca, daha akıllı kuyruk yönetimi sistemleri tasarlanabilir. Bu sistemler, ağ trafiğini dinamik olarak analiz ederek, en uygun kuyruk yönetimi algoritmasını uygulayabilirler. Örneğin, trafik yoğunluğu arttığında, kuyrukların dinamik olarak ayarlanması ve trafiği daha iyi yönetmek için akıllı bir kuyruk yönetimi sistemi kullanılabilir.

Son olarak, kuyruk yönetimi, ağ performansını artırmak için diğer teknolojilerle birleştirilebilir. Örneğin, trafik şekillendirme teknolojileri ile birleştirilerek, ağ trafiği daha verimli bir şekilde yönetilebilir. Ayrıca, kuyruk yönetimi teknikleri, paket işleme hızı, yönlendirme algoritmaları ve ağ topolojisi gibi diğer faktörlerle birleştirilerek, ağ performansını artırmak için daha kapsamlı bir yaklaşım kullanılabilir. Tüm bu alanlar, kuyruk yönetimi alanında gelecekteki araştırma ve geliştirme çalışmalarının odaklanabileceği konuları temsil etmektedir [7].

## 7.SONUÇ

Paket anahtarlama ağılar, günümüzün yüksek hızlı ve büyük ölçekli veri iletişimde önemli bir rol oynamaktadır. Ancak bu ağlarda veri trafiği yönetimi oldukça zorlu bir konudur ve kuyruk yönetimi performansı ağıın genel performansını belirleyebilir. Bu sebeple, ölçeklenebilir donanım öncelik sıralı kuyruk mimarileri, fairness kavramı, performans ölçümü ve değerlendirmesi gibi konular üzerinde araştırmalar devam etmektedir. Büyük ölçekli paket anahtarlama ağılarda ise kuyruk yönetimi zorlukları ve çözümleri üzerine çalışmalar yapılmaktadır.

Gelecekteki araştırma ve geliştirme alanları arasında, daha verimli kuyruk yönetimi algoritmaları, daha ölçeklenebilir ve düşük gecikmeli donanım mimarileri, ağda yaşanan trafiği daha iyi anlayıp yönetebilen yapay zeka teknikleri gibi konular yer almaktadır. Ayrıca, akıllı kuyruk yönetimi teknikleri, güvenlik açıklarının önlenmesi için kullanılabilir ve ağ yönetiminde kullanıcı deneyimini arttırmak için de faydalı olabilir.

Sonuç olarak, kuyruk yönetimi konusu, paket anahtarlama ağların performansı açısından oldukça önemlidir ve bu alanda yapılan araştırmalar, ağların daha verimli, güvenli ve ölçeklenebilir hale gelmesine katkı sağlayacaktır.

## 8.KAYNAKÇA

- [1] M. Zhu, H. Shen and Y. Fang, "Scalable hardware architectures for priority queue management in high-speed packet switches," in IEEE Transactions on Computers, vol. 54, no. 10, pp. 1250-1265, Oct. 2005, doi: 10.1109/TC.2005.166.
- [2] Mubashir, Sana. "Circuit Switching vs Packet Switching." Baeldung, 14 Nov. 2020, [www.baeldung.com/cs/circuit-switching-vs-packet-switching](http://www.baeldung.com/cs/circuit-switching-vs-packet-switching).
- [3] Maier, D., & Waldvogel, M. (2002). Fair queueing made simple. IEEE/ACM Transactions on Networking, 10(3), 357-366. DOI: 10.1109/TNET.2002.1002411
- [4] Elwalid, A., Mitra, D., & Soliman, H. (1993). Analysis of a backpressure-based packet switching system. IEEE Journal on Selected Areas in Communications, 11(9), 1435-1444.
- [5] Ma, W., Liu, J., & Liu, K. (2001). Queue management in large-scale packet-switched networks: challenges and solutions. IEEE Network, 15(3), 40-48. doi: 10.1109/65.923292
- [6] Suresh, S. (1993). A survey of scheduling and buffer management issues in packet switches and routers. IEEE Communications Magazine, 31(9), 42-50. doi: 10.1109/35.231570
- [7] Elmas, M. A. (2019). Queue Management in Computer Networks: Research Challenges and Future Directions. In Proceedings of the 2019 27th Signal Processing and Communications Applications Conference (SIU) (pp. 1-4). IEEE.
- [8] Elçi, A., Özgüner, F., & Özgüner, Ü. (2000). New hardware priority queue architectures for link scheduling in high-speed switches. IEEE Transactions on Computers, 49(11), 1236-1250.