T.C.

Trakya Üniversitesi

Mühendislik Mimarlık Fakültesi

Bilgisayar Mühendisliği Anabilim Dalı

Doç.Dr. Hasan Hüseyin BALIK

Dersin Adı

Paralel Mimariler

Sayısal Haberleşme

Konu

Kablosuz Ağ Protokolleri

Hazırlayan

Eser SERT

**ÖZET**

Kablosuz ağlar, iki yönlü olarak veri iletişimi sağlayan, iletim ortamı olarak fiber optik veya bakır kablo yerine radyo frekansı veya kızılötesi ışınları kullanan, salon, bina, kampüs vb. ortamlarda veri iletişimini sağlayan teknolojidir. Kurulum kolaylığı ve hareket serbestliği gibi önemli avantajlar sağlayan WLAN sistemleri kablolu ağların yerini alabilmekte hatta bu ağlara göre daha fazla fonksiyonlar içerebilmektedir.

Kablosuz iletişimde geliştirilen standartlar sayesinde kurallar açıkça ortaya konmuş buna bağlı olarak verinin hangi aşamalardan geçerek işleneceği, hareket edeceği vb. tüm noktalar ortaya konmuştur. Bu çalışmada kablosuz ağ, katman ilişkisi, ağlarda kullanılan protokoller, kablosuz ağ güvenlik protokolü, ağ türleri gibi konular anlatılacaktır.

**ABSTRACT**

Wireless networks provide two-way data communications and use radio frequency or infrared rays instead of fiber optic or copper cable for communication situation in living room, building campus and so on environments for providing communication technology. WLAN systems that provide such as important advantages as the ease of installation and mobility and they can get the location of wired networks even involve more functions according to these networks.

Owing to the standards developed by wireless communications, the rules have been clearly laid down and depending on this, all points of data have been revealed which stages it will be processed, will move and so on. In this study, such issues will be discussed as wireless network, the relationship between the layer, the protocols used in networks, wireless network security protocols, network types.

İçindekiler

[1. GİRİŞ 5](#_Toc292055688)

[2. OSI MODELİ AĞ SEVİYELERİNİN İNCELENMESİ 6](#_Toc292055689)

[2.1 Katmanlar 8](#_Toc292055690)

[2.2 OSI Modelinde Veri İşleme 11](#_Toc292055691)

[3. TCP/IP MODELLERİ 12](#_Toc292055692)

[3.1 Uygulama Katmanı 13](#_Toc292055693)

[3.2 İletim Katmanı 13](#_Toc292055694)

[3.3 İnternet Katmanı 14](#_Toc292055695)

[3.4 Ağ Arayüz Katmanı 14](#_Toc292055696)

[4. 802.11 STANDARDININ KATMANLARLA İLİŞKİSİ VE BAĞLANTI ÖZELLİKLERİ 15](#_Toc292055697)

[4.1 Kablosuz Ağlarda Katmanların İncelenmesi 15](#_Toc292055698)

[4.2. MAC erişim modları ve zamanlama 16](#_Toc292055699)

[4.3. Taşıyıcı Fonksiyonları Algılama ve Ağ Tahsis Vektörü 17](#_Toc292055700)

[4.4 Çerçeveler (Frames) Arası Boşluklar 19](#_Toc292055701)

[4.5. Parçalara Ayırarak (Fragment) Veriyi gönderme 21](#_Toc292055702)

[4.6. MAC Çerçeve Formatı 21](#_Toc292055703)

[4.6.1 Çerçeve Kontrol (Frame Control) 21](#_Toc292055704)

[4.6.2. Süreç/ ID (Duration/ID) 22](#_Toc292055705)

[4.6.3 Adres (Address Fields) 23](#_Toc292055706)

[4.6.4 Sıra Kontrol Alanı (Sequence Control Field) 23](#_Toc292055707)

[4.6.5 Çerçeve Kalıbı ( Frame Body) 23](#_Toc292055708)

[4.6.6 Çerçeve Kontrol Sırası (Frame Check Sequence) 23](#_Toc292055709)

[4.7. 802. 11 Standardında Haberleşme İşleminin Gerçekleştirilmesi 24](#_Toc292055710)

[4.8 802.11 İçinde Üst Kademe Protokollerinin İşlevi 25](#_Toc292055711)

[4.9 802.11e Hizmet Bakış Kalitesi ( Quality of Service Overview-QoS) 26](#_Toc292055712)

[5. BÜYÜKLÜKLERİNE GÖRE KABLOSUZ AĞLAR 28](#_Toc292055713)

[5.1. Kablosuz LAN Standartları 29](#_Toc292055714)

[5.1.1. IEEE 802.11a Standardı 33](#_Toc292055715)

[5.1.3. IEEE 802.11g Standardı 34](#_Toc292055716)

[5.1.4. IEEE 802.11n Standardı 34](#_Toc292055717)

[5.2. 802.11 Kablosuz Ağlarında Güvenlik Protokolü 43](#_Toc292055718)

[5.2.1 WEP (Wired Equivalent Privacy) 44](#_Toc292055719)

[5.2.2. Wi-Fi Korumalı Erişim (WPA) 45](#_Toc292055720)

[5.2.3. 802.1x 47](#_Toc292055721)

[5.2.4. WPA-2 Şifrelemesi (IEEE 802.11i) 48](#_Toc292055722)

[5.3. Diğer Kablosuz Ağlar 48](#_Toc292055723)

[5.3.1. Zigbee 48](#_Toc292055724)

[5.3.2.Bluetooth 50](#_Toc292055725)

[5.3.3.UWB 53](#_Toc292055726)

[5.3.4.WiMAX 54](#_Toc292055727)

[5.3.5.Mesh Network 56](#_Toc292055728)

[a. Mesh Networkler için Yönlendirme Protokolleri 57](#_Toc292055729)

[b. Dynamic Source Routing (DSR) Protokol 58](#_Toc292055730)

[6. KABLOSUZ SİSTEMLERDE YAYGIN OLARAK KULLANILAN CİHAZLAR 59](#_Toc292055731)

[6.1 Erişim Cihazları (Access Point-AP) 59](#_Toc292055732)

[6.2. Kablosuz Ağ Adaptörleri 60](#_Toc292055733)

[6.3. Bluetooth Aygıtı 60](#_Toc292055734)

[6.4. Ağ Genişletici Adaptör 61](#_Toc292055735)

[7. SONUÇ 62](#_Toc292055736)

[KAYNAKLAR 63](#_Toc292055737)

1. **GİRİŞ**

Kablosuz ağlar sayesinde, evde, işte, okulda, parkta vb. mekânlarda kablo sorunu olmadan ağa bağlanabilmekte, bilgiye kısa sürede sorunsuz ulaşılmaktadır. Bu ve benzeri avantajlarından dolayı günümüzde çok tercih edilen bir teknolojidir. Kablosuz ağ sistemi kullanıcılarına daha iyi hizmet verebilmesi için teknolojik özellikleri incelenmekte ve sürekli olarak geliştirilmektedir.

Kablosuz ağ sistemlerinde işlenecek verinin sistemin içinde hangi aşamalardan geçeceği, ne kadar veri işleme kapasitesine sahip olacağı, veri işleme hızı gibi konular IEEE (The Institute of Electrical and Electronics Engineers) tarafından geliştirilen standartlarla belirlenmiştir. Verinin hava yoluyla iletilmesinde ve alınmasında yine standartlara bağlı kalınmaktadır.

Kablosuz ağlarda veriler hava aracılığıyla gönderilip alındığından tehlikelere açıktır ve bunun içinde güvenlik protokolleri geliştirilmiştir. Bu protokoller sayesinde bilgiler şifrelenerek gönderilmekte ve dışarıdan gelecek saldırılara karşı önlem alınmaktadır.

1. **OSI MODELİ AĞ SEVİYELERİNİN İNCELENMESİ**

Bilgisayar ağlarının ilk kullanılmaya başladığı zamanlarda veri haberleşmesi için gerekli olan iletişim kurallarını her firma kendisine özgü olarak tanımlamaya çalışmıştır. Bu sebepten ilk zamanlarda bir karmaşa oluşmuş ve hazırladıkları ağ sistemleri sadece kendi aralarında haberleşebilmiştir. ISO(International Organization Standardization) tarafından OSI (Open System Interconnection) modeli tanımlanarak bu sorunların önüne geçilmiştir. Böylece farklı üreticiler aynı modeli kullandıklarından bu tür sorunlar ortadan kalkmıştır. OSI modeli, bir bilgisayar üzerindeki verileri ağ ortamı üzerinden diğer bilgisayar üzerindeki uygulamaya aktarılmasını sağlamaktadır (Demir, 2005).

OSI modeli, iki bilgisayar veya sistem arasındaki haberleşme için işlemleri katmanlar (layer) vasıtasıyla açıklamaktadır. Katmanlı model sayesinde iş bölümü yapılarak daha fonksiyonel bir şekilde işlemler yönetilebilir hale getirilmektedir. OSI’nin amacı ağ mimarilerinin ve protokollerinin bir ağ bileşeni gibi kullanılmasını sağlamaktır. ISO standardı ağ yönetimini 7 katmana ayırmıştır. İki bilgisayar sisteminin öncelikli olarak iletişim kurabilmesi için uygulama programını uygulama katmanında çalıştırır. Bu aşamadan sonra bilgi hiyerarşik olarak işlenerek fiziksel katmana kadar iletilmektedir. Fiziksel ortamdan sonrada iletim ortamına aktarılmaktadır. OSI modeli, donanıma göre değişiklik göstermemektedir. Fiziksel katman iletişimi sürdürebilmek için diğer birimlerde organizeli bir şekilde çalışmaktadır. Fiziksel katmanda değişik kablolama teknikleri kullanılabilmektedir. Bu sistemler iletişim tekniklerine göre farklıklar gösterebilmektedir. Her bir katmandaki işlemler birbirinden bağımsız fakat birbirinden haberdar olarak çalışmaktadır. (Demir, 2005).

Şekil 1.1’de gösterilen mimari ile Layer’lere baştanbaşa görevlerini taksim edilmiştir. Katman servisleri işlevlerini farklı katmanlar için tasarlanmış protokoller aracılığıyla gerçekleştirmektedir. Bitişik olmayan katmanlar arasında yasaklar ve bitişik katmanlar arasında iletişim prosedür çağrıları ve cevaplarıyla gerçekleştirilmektedir. Protokoller layer’ler arasında servislerin tekliflerini gerekli şekilde cevaplamaktadır. (Yuksel, 2010)

Bu katmanlı tasarım tüm sistemin anlaşılması için tasarımcılara gerekli soyut düşünceyi verir ve bu düşünceyle farklı katmanlarda tasarlanan protokoller üzerinde katman düşüncesine bağlı kalınır. Protokollerde referans mimarilerin kurallarına bağlı kalınmasıyla tasarlanırsa, tüm sistem uyumlu çalışacaktır.

Fiziksel (Physical)

Veri Bağı (Data)

Uygulama (Application)

Sunum (Presentation)

Oturum (Session)

Transport (Taşıma)

Ağ (Network)

Şekil 1.1.OSI Referans Modeli

* 1. **Katmanlar**

OSI modeli 7 adet katmandan oluşmaktadır. Bu katmanlar şekil 1.1.’de görüldüğü gibidir.

1. **Uygulama Katmanı (Aplication Layer)**

Uygulama programı ile bağlantı kuran katmandır. En üst kısımda bulunduğundan iletişim için kullanıcıya en yakın olan katmandır. Uygulama katmanı tanımlama bilgilerini ve tahsisini, aynı anda çalışan programların eş zamanlı olarak çalışmasını, hata düzeltmeleri için gerekli adımları içermektedir. Uygulama katmanı, ağ uygulamaları kullanan programlara arayüz desteği vermektedir.

1. **Sunum Katmanı (Presentatiton Layer)**

Bu katman sunulacak olan veriyi biçimsel olarak uygun şekle sokmakla sorumludur. Veri üzerinde biçimsel dönüşümler gerçekleştirmekle sorumlu bir katmandır. Sunum katmanı bir üstünde bulunan uygulama katmanından gerekli olan bilgiyi alır işledikten sonra ilgili katmana bilgiyi gönderir. Sunum katmanında temel olarak üç işlev gerçekleştirilir:

• Verinin formatlanması

• Verinin kodlanması

• Verinin sıkıştırılması (lerningnetwork.**cisco.com**, OSI Model Concepts)

Bir üst katmandan veriyi aldıktan sonra belirtilen fonksiyonlardan birisi yâda birkaçı veriye uygulanabilmektedir. İşlenmiş olan veri bir üst yâda alt katmana yönlendirilmektedir.

1. **Oturum Katmanı (Session Layer)**

İletişim kuracak iki düğüm arasında oturumun başlatılması sürdürülmesi ve sonlandırılması gerçekleştirilir. Aynı zamanda oturum başlatıldıktan sonra bağlantı yönetimi de bu katmanda gerçekleşir. İletişimin kopması durumunda devam etmesi için gerekli işlemler bu katmanda yürütülür.

1. **Ulaştırma Katmanı (Transport Layer)**

Ulaştırma katmanında, veri iletimi, veri akış kontrolü ve güvenliği sağlanmaktadır. Ağda taraflar arasında akış kontrolü sağlanmak için gerekli işlemler bu katmanda gerçekleşir. Bölünen parçalar veya paketler halinde veri akışında; alan bilgisayarın ulaştırma katmanı mesajı tekrar birleştirmektedir. Hatasız iletim için hata denetimi sürekli olarak gerçekleştirilmektedir. (lerningnetwork.**cisco.com**, OSI Model Concepts)

1. **Ağ Katmanı (Network Layer)**

Fiziksel adrese karşı, isimler ve mantıksal ağ adresleri dönüştürmektedir (örnek: bilgisayar ismi 🡺MAC adresi). Ağ katmanında, bilgi gönderim aşamasında en iyi yolun bulunması ve bu yoldan bilginin gönderilmesi sağlanmaktadır. Yönlendirici bilgisayarın göndereceği kadar büyük veri çerçevesi gönderemiyorsa, ağ katmanı küçük ünitelere bölerek dengeleme sağlamaktadır. Network katmanında bulunan IP (internet protocol) ile mantıksal adresleme işlemi gerçekleşir.

1. **Veri Bağı Katmanı (Data Link Layer)**

Veri bağı katmanı ağ üzerinde verinin formatını tanımlamaktadır Bir network bilgi çerçevesi, aka paketi, checksum içerikleri, kaynak ve hedef adresi içermektedir. Ağ ve fiziksel katman arasındaki bilgi çerçevelerini incelemektedir. Ağ katmanına teslim için veri çerçeveleri içine Fiziksel katmandan alınan paketler alınır. Bu katman network üzerinden alınan ve iletilen bilgileri tanımlar (lerningnetwork.**cisco.com**, OSI Model Concepts).

IEEE standartlarına göre veri bağı katmanı **LLC - Logical Link Control ve MAC – Media Access Control olmak üzere iki alt kategoriye (katmana) ayrılmaktadır.**

LLC alt katmanı bir üst katman olan ağ katmanı için geçiş görevi görür. Böylece, hata düzeltme ve akış kontrol yönetimi ve SAPs( Protokole özel mantıksal portlar) tanımlar. Bu standartlar 802.2 ile tanımlanmıştır. İkinci alt katman olan Media Access Control (MAC) ise, ağ adaptörü ile bağlantı kurarak verilerin aktarımını sağlar. Bu katman üzerinde çalışan donanımlardan olan anahtarlama ve veri köprüleme aygıtları verileri yönlendirmede ve filtrelemede MAC adreslerini kullanır.

1. **Fiziksel Katman (Physical Layer)**

Bakır tel yâda hava gibi fiziksel bir ortam üzerinde bit iletimi için mekanik ve elektriksel özellikleri tanımlamaktadır (Marsic, 2010). Diğer katmanlar dijital olarak çalışırken fiziksel katman dijital bilgileri dış ortama aktarmak için nasıl elektrik, ışık yâda radyo sinyallerine çevrilip aktarılacağını standartlar aracılığıyla tanımlamaktadır.

Şekil 1.2.’de bilgilerin katmanlar arasında işleme tabi tutulurken biçimsel olarak almış olduğu değişiklikler görülmektedir. Örneğin Uygulama katmanından sunum katmanına giden bir paketin başına AH(Application Head) geldiği görülmektedir. Data katmanında ise gerektiğinde data link trailer (DT) eklenebilmektedir. Bunun amacı ise data senkronizasyonunu sağlamaktır.

Şekil 1.2. Katmanlarda Başlık Eklenmesi (www.microsoft.com)

Gönderme Süreci

Protokolü

Data link

Alma Süreci

Application

Presentation

Session

Transport

Network

Data

Physical

Application

Presentation

Session

Transport

Network

Data

Physical

Veri

Veri

AH

Veri

AH

PH

Veri

AH

PH

SH

Veri

AH

PH

SH

TH

Veri

AH

PH

SH

TH

NH

Veri

AH

PH

SH

TH

NH

Veri

AH

PH

SH

TH

NH

DH

DH

DT

DT

Uygulama Protokolü

Sunum Protokolü

Oturum Protokolü

İletim Protokolü

Network

Protokolü

Bitler

Gerçek veri iletim yolu



## OSI Modelinde Veri İşleme

Ağ içerisinde haberleşmeler hedef ve kaynaklar arasında gerçekleşmektedir. Bilgi ya veri yâda veri paketleri olarak indirilmektedir. Bir bilgisayar başka bir bilgisayara veri göndermesi için verinin ilk başta encapsuling işleminden geçmesi gerekmektedir. Encapsuling işlemi sayesinde gerekli protokoller veriye uygulanıp hareket ettirilmektedir.

Veri alt katmanlara iletilirken iletim şekli şu şekilde olur: Veri (data) halinde alınan bilgi, taşıma katmanında kesim (segment) adı verilen birimlere ayrılır. Bu şekilde veri alıcı makinede tekrar bir araya getirilirken doğru sıralanması sağlanmış olur. Ağ katmanına segment şeklinde gelen verilere burada adres bilgileri eklenir; böylece kesimler paket haline dönüşür. Veri-bağlantı katmanında paketlere MAC adresleri eklenerek çerçeve (frame) yapı oluşur. En son aşama olarak fiziksel katmana gelen çerçeveler burada bir bit dizisine dönüştürülerek iletime hazır hale getirilir.

1. **TCP/IP MODELLERİ**

Günümüzde internetin temel protokolü olarak yerini almış olan TCP/IP’nin açılımı Transmission Control Protocol/Internet Protocol‘dür. Bu protokol Birleşik Devletlerde doğmuştur. Bu ağ mimarisi katmanlı yapıda olup, bilgisayarlar arası iletişim için gerekli bütün iş bu dört katmandan yürütülmektedir.

• Uygulama katmanı

• Taşıma katmanı

• İnternet katmanı

• Ağ erişim katmanı

TCP/IP protokol mimari yapısı üzerinden ağ için ISO/OSI mimarisi iyi bir tasarım için başarılı bir örnektir (Da˜nobeitia-Paul B., Ferrer-Gomila J.L. vd., 2008). Dolayısıyla iki mimaride birbirini destekleyen ve katmanlı bir şekilde tasarlanan önemli modellerdir.

Günümüzde internetin temel protokolü olarak yerini almış olan TCP/IP’nin açılımı Transmission Control Protocol/Internet Protocol‘dür. Bu protokol Birleşik Devletlerde doğmuştur. Bu ağ mimarisi katmanlı yapıda olup, bilgisayarlar arası iletişim için gerekli bütün iş bu dört katmandan yürütülmektedir

UYGULAMA (APPLICATION)

TAŞIMA (HOST TO HOST)

İNTERNET (INTERNET)

AĞ ARAYÜZ (NETWORK INTERFACE)

Şekil 3.1. TCP/IP Modeli (TCP/IP Overview, Cisco, 2005)

TCP/IP modelinin yapısı itibariyle OSI gibi katmanlar halinde tasarlanmıştır. TCP/IP, temelde TCP (Transmission Control Protocol – İletim Kontrol Protokolü) ve IP (Internet Protocol – İnternet Protokolü) olmak üzere iki ana protokolden oluşur. Bilgiler paketlenirler ve TCP bu paketlerin iletilmesinden, IP ise bu paketlerin yönlendirilmesinden sorumludur.

## 3.1 Uygulama Katmanı

Uygulama katmanında bulunan protokoller sayesinde uygulama programları ile iletişim kurmaktadır. Bu katmanda işlemlerin yapılabilmesi için bir alt katmandan hizmet beklenmektedir.

SNMP (Simple Network Management Protocol-Basit Ağ Yönetim Protokolü): Ağ sisteminde bulunan, yönlendirici (router), anahtar (switch) ve hub gibi cihazların yönetimini sağlar. SNMP desteği olan ağ cihazları SNMP mesaj alışverişi ile uzaktan yönetilebilir.

TELNET (Telecommunication Network-İletişim Ağı): Kullanıcının, herhangi bir makineye sanki o makinenin istasyonuymuş gibi iletişim kurmasını sağlayan protokoldür.

FTP (File Transfer Protocol-Dosya Aktarım Protokolü): Ağ sistemiyle bağlı olan iki bilgisayar arasında dosya aktarımının yapılmasını sağlayan protokoldür. İnternet üzerindeki iki sistem arasında dosya aktarımı için kullanılan temel protokoldür.

NNTP (Network News Transport Protocol-Ağ Haberleri Aktarım Protokolü): USENET postalanma hizmetinin yürütülmesini sağlar.

HTTP (The Hypertext Transfer Protocol-Yüksek Metin İletişim Protokolü): Web sayfalarının alışverişini sağlar. (TCP/IP ve IP Adresleme, 2008, MEGEP)

## 3.2 Taşıma Katmanı

TCP ve UDP (User Datagram Protocol- Kullanıcı Veri Bloğu Protokolü) ulaşım katmanı protokolleri olup, bir üst katmandan gelen veriyi paketleyip bir alt katmana gönderir. TCP, uçlar arası veri dağıtımını sağlamakla birlikte verinin güvenli bir şekilde dağılabilmesi için gerekli fonksiyonları içermektedir. Bunlar, hata denetimi, sıra numarası, onay ve yeniden gönderim olmak üzeredir. TCP bağlantı yönlü bir protokoldür. Bu protokol segment denen uygulama katman bilgilerini sürdürürken kaynak ve hedef arasındaki iletişimi devam ettirmektedir. İletim katmanında bulunan diğer bir protokol olan UDP ise, veri iletimi gerçekleştirilmesinde rol oynamakla birlikte bu işlem sırasında paketlerin ulaşacağını garanti etmemektedir. Çünkü akış kontrolü bu protokolde gerçekleştirilmemektedir.

## 3.3 İnternet Katmanı

IP internet İnternetle üçüncü katmanda bulunmaktadır. IP hata raporlamaları, parçalama ve farklı maksimum data ünite boyutlarıyla ağlar üzerinde iletim için bilgi ünitelerinin ilgili datagramını düzenler (TCP/IP Overview, Cisco, 2005).

İnternet katmanı protokollerinden olan, ARP (Adres Çözümleme Protokolü), bir IP adresinin hangi ağ kartına (yani MAC adresine) ait olduğunu bulmaya yarar. TCP/IP'de veri gönderiminde gönderilecek bilgisayarın hangisi olduğunu bulmak için kullanılır.

Bir diğer internet katmanı protokolü olan RARP (Ters ARP), ARP'ın tersi işlemi yapar, yani hangi MAC adresinin hangi IP adresini kullandığını bulur. Bir TCP/IP ağında RARP'ın çalışacağı garanti değildir, zira RARP bir RARP sunucusuna ihtiyaç duyar.

Yönlendirme katmanında tanımlı ICMP protokolü kontrol amaçlı bir protokoldür. Genel olarak sistemler arası kontrol mesajları ICMP protokolü üzerinden gönderilir.

## 3.4 Ağ Arayüz Katmanı

OSI modelindeki Fiziksel Katmana karşılık gelmektedir. IP paketlerinin ihtiyacı olan fiziksel bağlantıları kurmak için gereken bağlantıyı kurmada rol oynamaktadır.

Uygulama katmanında bulunan protokoller, FTP, HTTP, SMTP, DNS, TFTP .

İletim katmanı için, TCP, UDP.

İnternet katmanı için, ARP, RARP, IP, ICMP

Network Acess için, ETHERNET, Token Ring, FDDI…

# 4. 802.11 STANDARDININ KATMANLARLA İLİŞKİSİ VE BAĞLANTI ÖZELLİKLERİ

## 4.1 Kablosuz Ağlarda Katmanların İncelenmesi

IEEE 802.11 standardı kablosuz istasyonlar ve kablolu network altyapısının bağlantısını geliştirmek için kullanılan önemli bir iletişim standardıdır. IEEE 802.11 protokolü ve bağlantı teknolojisi aracılığıyla toplantı odaları, koridor, lobiler, kafetaryalar vb. mekanlarda ağ erişimi sağlanabilir. 2. konuda anlatılan OSI modeli bağlı kalınarak kablosuz mimariyle çalışan sistemlerin tasarımı yapılabilmektedir.(Gast,2002)

Şekil 4.1.’de gösterildiği gibi, kablosuz ağlar farklı yapılara sahip olabilirler. Bazılarında ortam bir Access point istasyonu tarafından yönetilir, bazılarında ise bilgisayarlar birbirlerine kablosuz bağlantıyla bağlanabilir. 802.11 standartları her iki konfigürasyonu da dikkate alacak şekilde tasarlanmıştır.

Access Point



Şekil 4.1. Acess Point’li ve Ad-Hoc yapısındaki kablosuz ağlar (Marsic, 2010)

802

Mimarisi

802.1

Yönetim

802.3 MAC

802.3

PHY

802.11 MAC

802.5 MAC

802.5

PHY

802.11 FHSS PHY

802.11 DSSS PHY

802.2 Lojik bağlantı kontrolü (LLC)

802.11a

OFDM PHY

DİĞERLERİ

Data Bağlantı LLC alt katmanı

MAC altkatmanı

Fiziksel katman

Şekil 4.2. Ağ ortamında Protokol genişlemesinin dinamik oluşumu

IEEE 802 özellikleri OSI modelinin iki alt katmanı üzerinde odaklanmıştır, çünkü OSI model fiziksel ve data katmanları birlikte çalışmaktadır. MAC, data göndermek ve erişim araçlarının nasıl düzenleneceğinin kurallarını ayarlar, fakat iletişimin detayları ve kabulü PHY’ye bırakılmıştır.

802 serisinin bireysel özellikleri ikinci numarasıyla düzenlenmiştir. Örneğin 802.3, Ethernet’le ilgili çarpışma algılama (Collision Detection-CSMA/CD ) ile Carrier Sense Multipli Access network olarak isimlendirilmiştir ve 802.5 Token Ring’dir. Diğer özellikler 802 protokol katmanının başka kısımlarını oluşturmaktadır. 802.2 herhangi bir düşük katman LAN teknolojisinde kullanılabilecek LLC, ortak bir link katmanıdır. 802 ağları için yönetimsel özellikler 802.1’de tanımlanmıştır. 802.1’in çok sayıda hükümleri arasında, köprüleme(802.1d) ve sanal LAN’lar veya VLAN’lar (802.1d) bulunmaktadır. (Gast, 2002)

OSI modelinin temel tanımlamaları yapılırken, fiziksel katmanın üst katmanlardan gelen veriyi elektriksel formata çevirerek bit formatında iletmekte olduğu tanımlanmıştı. 802.11 kablosuz protokol standardını belirttiği için verinin radyo sinyalleriyle gönderileceğini vurgulamaktadır. Şekil 4.2.’de 802.11, 802.11a, 802.11b olarak kablosuz ağ türleri sıralanmıştır. Burada sona gelen a, b gibi ifadeler kablosuz ağın teknolojik özelliğini belirtmektedir. Buna göre, fiziksel katmanda kullanılacak modülasyon teknikleri değişeceğinden şekil 4.2.’de frequency hopping spread-spectrum (FHSS), a direct-sequence spread-spectrum (DSSS) vb. kullanılmıştır. Diğerleri olarak belirtilen, 802.11g DSSS/OFDM, 802.11n MIMO/OFDM kullanmaktadır.

802.11 kablosuz iletişim modelinde veriler karşıya MAC adreslerine göre teslim edilecekleri için fiziksel katman ile MAC katmanı organizeli çalışmaktadırlar.

## 4.2. MAC erişim modları ve zamanlama

Kablosuz erişim modları koordinasyon fonksiyonları ile kontrol edilmektedir. Ethernete benzer şekilde CSMA/CA erişimi dağıtılmış koordinasyon erişimi (disrubted coordination function (DCF)) aracılığıyle geliştirilmiştir. (Gast, 2002)

DCF kullanıldığında, CSMA/CA (CSMA/Collision Avoidance) mekanizması çalıştırılır. Veri göndermek isteyen istasyon ortamı dinler, ortam boş ise veri gönderilir, ortam meşgul ise beklenir. Ancak veri gönderilirken ortam dinlenemediği için oluşan çakışmalar o anda anlaşılmaz. Çakışma durumunda ikili geri çekme algoritması çalıştırılmaktadır. DCF’de Ortama erişmek için istasyona ne kadar beklemesi gerektiğini bildirir ve veri çakışmalarının engellenebilmesi için zamanlayıcılarla sistem kontrol altına alınmıştır.

802.11 standardının desteklediği diğer operasyon ise PCF’dir. Bu ise, merkezi kontrol tekniği olarak isimlendirilebilmektedir. PCF Access point içinde nokta koordinatörlerini bulundurur, bunun için network yapısında PCF network yapısıyla sınırlıdır. Çekişme tabanlı servisler üzerinden öncelik kazanmak için, PCF istasyonları kısa bir aradan sonra çerçeve iletimini gerçekleştirmektedir.

## 4.3. Taşıyıcı Fonksiyonları Algılama ve Ağ Tahsis Vektörü

Taşıyıcı algılama, ortam müsaitse düzenlemek için kullanılmaktadır. 802.11 yönetiminde bu süreç iki tip taşıyıcı algılama fonksiyonuna sahiptir: fiziksel taşıyıcı algılama ve sanal taşıyıcı algılama olmak üzeredir. Taşıyıcı algılama fonksiyonu ortamın meşgul olduğunu belirtirse, MAC raporcusu üst katmanlara bu durumu iletmektedir.

Fiziksel taşıyıcı algılama fonksiyonları söz konusu fiziksel katman aracılığıyla ve ortama bağlı olarak modülasyon kullanarak geliştirilir. Dolayısıyla bu zordur. Sanal taşıyıcı algılama ağ tahsis vektörü üzerinden geliştirilmiştir. En sık olarak 802.11 çerçeveleri, belli bir zaman için ayrılmış olarak kullanılabilir bir sürede taşır. NAV ortalama tahsis edilen zamanı göstermektedir.

Şekil 4.3.’de CSMA/CA prensibine bağlı olarak ağda bulunan iki bilgisayarın kablosuz şekilde haberleşmesi sinyallerle açıklanmaktadır. Şekil 4.4.’de ise bu sistemin çalışmasını açıklamak için sinyal modellemesi yapılmış ve açıklanmıştır.

Şekil 4.3.’deki sistemde, veri çerçevelerin rasgele erişiminden ziyade, göndericinin kanal ayırmasına izin verir.



RTS

CTS

data

ACK

SIFS

SIFS

SIFS

DIFS

Gönderici

Alıcı

*Şekil 4.3. Ağda gönderici ve alıcı ilişkisi (Gast, 2002)*

*Request to send (RTS) : Gönderim isteği*

*Clear to send (CTS): Gönderime uygun*

*Network Allocation Vector (NAV): Ağ tahsis vektörü*

*Short Inter-Frame Space* (*SIFS):Kısa dahili çerçeve mesafesi*

*Distributed Inter-Frame Space* (*DIFS):Dağıtılmış dahili çerçeve mesafesi*

RTS

ÇERÇEVE

Gönderici

CTS

ACK

Alıcı

NAV(RTS)

NAV(CTS)

NAV

SIFS

SIFS

SIFS

DIFS

Şekil 4.4. CSMA/CA haberleşmesi (Gast, 2002)

Bu modda gönderen ve alıcı arasında veri iletimi öncesinde bir haberleşme gerçekleşir. Bu haberleşmeyi duyan diğer istasyonlar da uygun şekilde davranırlar. Gönderici RTS sinyalini gönderdikten sonra SIFS süreci devreye girer. Burada SIFS onay çerçevelerinde kullanılır. Sadece kendine gönderilmiş bir çerçeve alan uç SIFS süresi içinde ***onay*** gönderir. Dolayısıyla SIFS sürecinden sonra, alıcı talebi kabul ederse gönderime uygun sinyali olan CTS’yi gönderilir. CTS’den sonra gönderici SIFS süresi kadar bekleyip çerçeveyi gönderir. Göndericinin çerçeve gönderimi bittikten sonra SIFS süreci geçer ve alıcı bilgileri başarıyla almışsa ACK sinyalini gönderir. Şekil 4.4’de görülen NAV’larla istasyonların bağlantılarının kesintiye uğramasının önüne geçilmiştir.

## 4.4 Çerçeveler (Frames) Arası Boşluklar

Geleneksel Ethernet, iletim ortamında koordinasyonu sağlamada büyük bir rol oynar. 802.11 dört farklı dahili çerçeve kullanmaktadır. Bunlardan SIFS, PIFS ve DIFS ortam elverişliliğini düzenlemek için kullanılmaktadır. EIFS’de kötü çerçeve durumları için kullanılan bir mekanizmadır.

ACK

SIFS

Alıcı

Alıcı

PIFS

DIFS

Çerçeve Aktarımı

Çekişme

Periyodu

Erteleme Erişimi

İkili üstel geri çekilme kullanarak

slot seçimi

Şekil 4.5. Dahili çerçeve boşluklarının ilişkisi (Marsic, 2010)

SIFS (Kısa Dahili Çerçeve Aralığı- Short InterFrame Spacing) :SIFS, kontrol çerçeveler gibi yüksek öncelikli yayınlarda ya da tek bir iletişime ait yayılmış yayınlar için (Örneğin ACK çerçeve parçası) kullanılır. Bu değer PHY başına sabittir ve iletim istasyonu, alış modunda geri dönebilecek ve kodları çözülmüş paketlerin kapasitesinde olacak şekilde hesaplanacaktır. 802.11 için FH PHY değeri 28 mikrosaniyedir. (Marsic, 2010)

PIFS (PCF Dahili Çerçeve Boşluğu-PCF InterFrame Spacing): PIFS çekişme-boşluk işlemi sırasında PCF aracılığıyla kullanılmaktadır. Koordinatör istasyon yoklamaları düzenlemede PIFS kullanır ve yoklama istasyonu SIFS bekleme süresi ve çekişme tabanlı trafikte önceden ayrılan kadar beklemeden sonra iletebilir.(Marsic, 2010)

DIFS (DCF Dahili çerçeve Boşluğu- DFC InterFrame Spacing): DIFS erişim için asenkron çerçevelerin çekişmesine uygun minimum ve orta zamandır. DIFS’den daha uzun bir periyot hat boşsa istasyonlar acilen erişirler. Çakışmaları engellemede önemli bir boşluk türüdür.

EIFS (Genişletilmiiş Dahili çerçeve Boşluğu- Extended InterFrame Spacing): EIFS diğer istasyon boşluklarından daha uzundur. EIFS bazı istasyonlardan bozulmuş ya da bilinmeyen bir çerçeve almış bir istasyon tarafından kullanılır.

## 4.5. Parçalara Ayırarak (Fragment) Veriyi gönderme

Kablosuz olarak verinin taşınması sırasında hatalar oluşabilmektedir. Uzun veri bloklarının hata taşıma olasılıkları fazladır. Bu nedenle kablosuz ortamda verinin kısa çerçeveler içinde taşınması daha az hata doğuracaktır. Uzun bir veri bloğu parçalara (fragments) bölünür ve bu şekilde gönderilir. Eğer veride bir hata oluşsa yalnızca hatalı parçanın gönderilmesi yeterli olacaktır. Bu durumda NAV’ın kullanılması sadece ilk çerçeveyi koruyacaktır. Bu durum Şekil 4.6.’de sinyallerle anlatılmıştır.

DIFS

SIFS

RTS

Gönderici

Alıcı

SIFS

CTS

Fragment 0

ACK 0

SIFS

SIFS

Fragment 1

ACK 1

SIFS

SIFS

RTS

CTS

ACK 0

Fragment 0

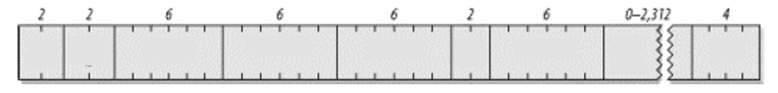
zaman

NAV

Şekil 4.6. Veri parçalama yapısı (Gast, 2002)

## 4.6. MAC Çerçeve Formatı

MAC çerçeveleri kablosuz veri bağlantısındaki zorlukları karşılamak için en az dört adres çerçevesi, ve diğer önemli bitleri ile data katmanında önemli işlevleri üstlenmektedir. MAC elemanında oluşan çerçevenin yapısı şekil 4.7.’de görüldüğü gibidir.



FCS

Frame

Body

Adres 1

Adress 2

Adress 3

Adress 4

Frame Control

Duration

/ID

Seq

ctl

Şekil 4.7. 802.11 MAC çerçeve yapısı (Gast, 2002 ve Marsic, 2010)

### 4.6.1 Çerçeve Kontrol (Frame Control)

Şekil 4.7.’de görülen MAC çerçeve yapısında, ***çerçeve kontrol’*** un iki baytıyla başlamaktadır Çerçeve kontrol içinde Protocol (2 bit), Type=data (2 bit) , Sub type (4 bit), to DS (1 bit), from DS(1 bit), Retry(1 bit), Pwr Management(1 bit), More Data(1 bit), WEP(1 bit), Order(1 bit) gibi bitler vardır. Frame kontrol içindeki bitlerin toplamı 16 bit=2 Byte’dır Dolayısıyla MAC çerçeve yapısında da 2 Byte olarak alan tahsisi yapılmıştır.

**Protocol Version:** 802.11 MAC versiyonu çerçevede bulunan iki bitle gösterilmektedir.

**Type and subtype fields:** Bu alan kullanılan çerçevenin türünü belirtmek için kullanılmaktadır. Karmaşanın önüne geçebilmek için bu alan tasarlanmıştır.

**ToDS and From DS bits:** Dağıtım sistemlerine bir çerçevenin yöneltilip yöneltilmeyeceğini belirtir.

**More Fragments:** Bu bit fonksiyonları, daha çok IP içindeki “daha fazla kısımlara (more fragments)” benzer. Yüksek seviyeli bir paket MAC aracılığıyla parçalandığında, ilk kısmı ve bazı izleyen sonlanmayan parçaları 1’e bu bit ayarlar.

**Power Management:**802.11 üzerinden çalışan ağ adaptörlerinde çoğunlukla yerleşik bir pille çalışan sistemler, bir dizüstü veya el bilgisayarı kullanır. Pille ilgili durumların kontrolleri bu alanla koordine edilmektedir.

**More Data Bit:** Güç tasarruf modunda istasyonları yerleştirmek için, dağıtım sistemlerinden alınan erişim noktaları tampon olarak kullanılabilmektedir. Bir Access point’de en az bir çerçevenin olduğunu göstermek için bu bit ayarlanır ve bekleyen istasyon adreslenir.

**WEP bit:** Kablosuz iletişimi kesmek sabit bir ağ üzerinde iletimi kesmekten daha kolaydır. 802.11 kimlik verilerini korumak için Wired Eqivalent Privacy (WEP) şifreleme yordamını çalıştırmaktadır.

**Order Bit:**Çerçeveler ve parçalar, gönderilen ve alınan MAC’ların her ikisinin aracılığıyla ek işlenmesine bağlı olarak sıralı işlenmektedir.

### 4.6.2. Süreç/ ID (Duration/ID)

Duration/ID alanı çerçeve kontrol alanını izlemektedir. Süreç yani işlem akış zamanlamaları üzerinde önemlidir.

### 4.6.3 Adres (Address Fields)

Bir 802.11 çerçevesi 4 adres alanı içermektedir. Adres alanları numaralandırılmıştır, çünkü farklı alanlar çerçeve tipleri üzerinden farklı öneriler yapmaktadır. Bunlar varış(destination) adresi, kaynak (source), alıcının (receiver) adresi, verici(transmitter) adres olmak üzeredir.

### 4.6.4 Sıra Kontrol Alanı (Sequence Control Field)

Bu kontrol alanı 16 bit içermekle birlikte birleştirme ve çift çerçeveleri ayırmada kullanılmaktadır. Sıra kontrol alanı, 4 bit parça numara alanı, 12 bit sıra numara alanıdır.

### 4.6.5 Çerçeve Kalıbı ( Frame Body)

Data field olarak da anılan, çerçeve kalıbı (frame body) istasyondan istasyona üst katman yüklerini taşımaktadır.

### 4.6.6 Çerçeve Kontrol Sırası (Frame Check Sequence)

Ehernet’li 802.11 çerçevesi bir çerçeve kontrol dizisi (FCS)’ye bağlıdır. FCS matematik operasyonları temel aldığından döngüsel atıklık denetiminden (CRC) yararlanmaktadır.

## 4.7. 802. 11 Standardında Haberleşme İşleminin Gerçekleştirilmesi

RTS

ÇERÇEVE

Gönderici

CTS

ACK

Alıcı

NAV(RTS)

NAV(CTS)

NAV

SIFS

SIFS

SIFS

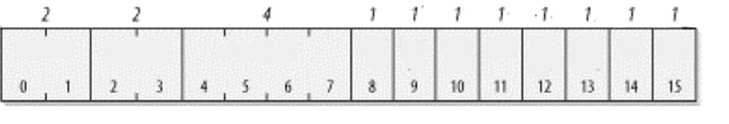
DIFS

Şekil 4.8. Veri haberleşmesi

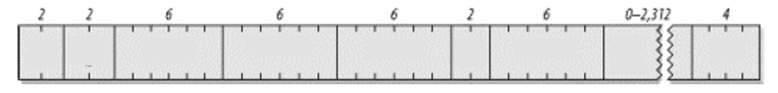
Şekil 4.8.’de görülen RTS sinyalini göndermek için, Data katmanına bulunan MAC çerçevesine bağlı çerçeve kontrol sinyallerinden Type:01,Sub type:1011 olacak şekilde kurulur.

CTS sinyali için: Type:01,Sub type:1100

ACK sinyali için: Type:01,Sub type:1101, şeklinde olacaktır. Bu durum şekil 4.9.’da gösterilmiştir. (Gast, 2002)



Protokol



FCS

Frame

Body

Adres 1

Adress 2

Adress 3

Adress 4

Frame Control

Duration

/ID

Seq

ctl

Type

Sub Type

To Ds

FromDs

More Frag

Pwr Mngmt

Retry

More Data

WEP

Order

1

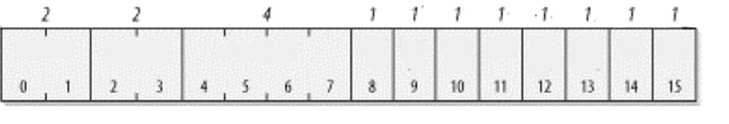
0

1

1

0

1



1

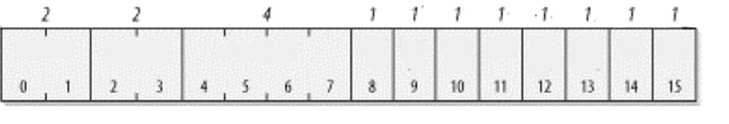
0

0

0

1

1



1

0

1

0

1

1

RTS

CTS

ACK

**802.11 MAC FRAME**

**FRAME CONTROL**

Şekil 4.9. MAC çerçevesi ve Çerçeve kontrol (Gast, 2002)

## 4.8 802.11 İçinde Üst Kademe Protokollerinin İşlevi

Destination MAC

Source MAC

Type 0x800 (IP) 0x806(ARP))

IP Packet

FCS

802.11 MAC başlıkları

SNAP DSAP 0XAA

SNAP SSAP 0XAA

Control 0x03(UI)

RFC 1042 encapsuling

Type

IP packet

FCS

24 veya 30

802.11

Ethernet

6

6

2

variable

4

SNAP Header

Copy

Copy

Tekrar Hesapla

Şekil 4.10. 802.11 içinde IP kapsüllemesi (Gast, 2002)

MAC adresleri kapsül çerçevesine eklenir, ve o zaman bir alt servis network protokol (SNAP) başlığı eklenir. SNAP başlıkları bir hedef servis Access point (DSAP) ile ve bir kaynak servis Access pointiyle başlar. Adreslerden sonra, SNAP kontrol başlıkları içerir. Yüksek seviye data bağlantı kontrolü (HDLC)’ne benzemektedir ve kontrol alanı numaralandırılmamış bilgi (UI) için 0x03’e kurulur. (Gast, 2002)

Yönlendirme

C3

Yönlendirme

C3

Yönlendirme

C3

Yönlendirme

C3

Data Bağlantısı MAC

Fiziksel

Network

Ulaştırma

Yönlendirme

Çekişme/ Tıkanıklık Kontrol

Güvenilirlik

Şekil 4.11. Katmanlar arası veri akışı (Lim, Luo vd., 2006)

Şekil 4.11’de ulaştırma katmanından yola çıkan verinin kablosuz router’lardan geçerek hedefe ulaşması gösterilmektedir.

## 4.9 802.11e Hizmet Bakış Kalitesi ( Quality of Service Overview-QoS)

Bu konuda network sistemlerinde kalite servislerinin önemi üzerinde durulacaktır.

NETWORK

Paketler



Paketler

Görüntü ve Ses

Şekil 4.12. Multimedya bilgisinin kavramsal olarak modellenmesi (Marsic, 2010)

Şekil 4.12’de network üzerinde multimedya bilgisinin iletimi kavramsal olarak modellenmiştir. Burada kamera ve mikrofon gibi fiziksel ortamlardan alınan veriler network ortamında iletilmektedirler. İletim aşamasında kayıp vermeden yüksek veri oranıyla hedefe verileri iletmektir. Bu durumda kapasite ve gecikme sınırlamalarından servis kalitesi kavramı doğmuştur. Servis kalitesi ile veriler optimum dengeyle iletilmeye çalışılmaktadır. İlk başta bilgilerin nitelikleri değerlendirilir daha sonra ise servisler devreye girerek belirlenmiş öncelik sırasına göre hedefe iletilmektedir. (Marsic, 2010)

Kaynak

Ortam

Örnek:

İletim Kanalı

Hedef

**Parametreler:**

Kaynak bilgi oranı

İstatistiksel karakteristikler

**Parametreler:**

Servis kapasitesi

Servis kalite listesi

* Bekletme seçimleri
* Bilgi kaybı seçimleri

**Parametreler:**

Gecikme sınırlamaları

Bilgi kaybı toleransı

Şekil 4.13. Servis kalitesinde önemli faktörler (Marsic, 2010)

Wi-Fi tarafından servis kalitesinin sağlanması için kablosuz medya (WMM) 802.11e standardı ile kullanılmaktadır. WMM, verileri ses, video, best effort ve arka plan olarak değerlendirerek öncelik sırasına göre veri trafiğini yönetir. Böylece IEEE **802.11e** ile birlikte gelen yeni özellikler ile kablosuz ağlarda servis kalitesinin sağlanmaktadır.

# 5. BÜYÜKLÜKLERİNE GÖRE KABLOSUZ AĞLAR

Kablosuz ağlar kapsama alanlarına göre sınıflandırılabilmektedirler. Fakat Kablosuz ağ teknolojilerindeki gelişmeler ve kapsama alanını sınıflandırmadaki zorluklar nedeniyle sınırlandırma işlemini yapmayı zorlaştırmaktadır. Kablosuz iletişim ağları 4 sınıfa ayrılabilmektedir, bunlar:

* Kablosuz Geniş Alan Ağları (Wireless Wide Area Networks, WWAN),
* Kablosuz Metropol Alan Ağları (Wireless Metropolitan Area Networks, WMAN)
* Kablosuz Yerel Alan Ağları (Wireless Local Area Networks, WLAN) ve
* Kablosuz Kişisel Alan Ağları (Wireless Personal Area Networks, WPAN)

Olarak sıralanabilir. Şekil 5.1.’de kablosuz ağların sınırları verilmiştir.

**MAN**

<15 km

MobileFi -802.20

1 Mb/s

**MAN**

<5 km

WiMAX – 802.16 a / e

70 Mb/s

**LAN**

<100m

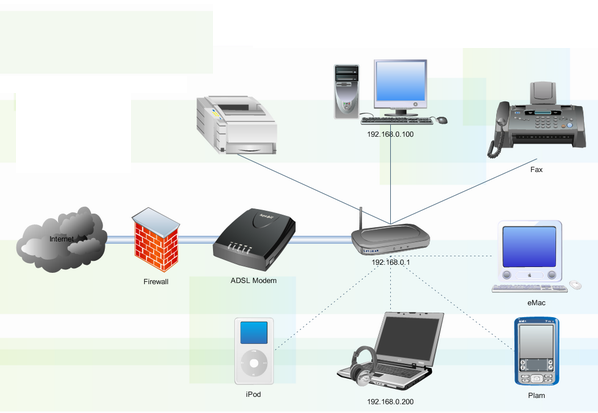
WiFi – 802.11 a/b/g/n

1-300 Mb/s

Şekil 5.1. Kablosuz ağların büyüklüklerine göre sınıflandırılması (Howlader ve Kiger, 2007)

**5.1. Kablosuz LAN Standartları**

Kablosuz ağlar içinde önemli bir yere sahip olan LAN’lar genelde kafeterya, bina içi, iş yerleri vb. alanlarda 0-100m kapsama alanına bağlı olarak çalışmaktadırlar. İki yönlü olarak veri iletişim desteği sağlamaktadırlar. Fiziksel donanım olarak fiber optik veya bakır kablo yerine radyo frekansı veya kızılötesi ışınları kullanarak belirlenmiş alanda iletişim sağlamaktadırlar. WLAN sistemleri günümüzde hızlı bir şekilde gelişmekte ve yeni fonksiyonlar eklenmektedir. Kablosuz yerel ağlar, yaygın olarak Wi-Fi olarak adlandırılmaktadır (Wireless- Fidelity – Kablosuz Bağlılık), RLAN (Radio Local Area Network), WLAN(Wireless LAN) olarak adlandırılmaktadırlar.



Şekil 5.2. Kablosuz ağ sistemi

WLAN sistemlerinde farklı teknolojilerde göze çarpmaktadır. Bunların başında, az da olsa kızılötesi (Infrared, Irda) teknolojisi de kullanılmaktadır. Kızılötesi sistemler; görünür ışığın hemen altındaki kızılötesi ışınları kullanarak veri iletişimi gerçekleştiren teknolojiye sahiptir. WLAN alanında kullanılan kızılötesi sistemi ile çalışan cihazlar muhakkak birbirlerinin görmelidirler. Ayrıca iletişim mesafesi de yaklaşık 10 metre olduğundan oldukça kısadır. Bu tür sorunları nedeniyle kızılötesi sistemler yaygın olarak kullanılmamaktadır.

Kablosuz WLAN çalışmalarında IEEE (Elektrik ve Elektronik Mühendisleri Enstitüsü-Institute of Electrical and Electronic Engineers) standart geliştirerek bu teknolojinin daha fonksiyonel olarak kullanılmasını sağlamıştır. İlk olarak IEEE 802 LAN/MAN standart komitesi 1997’de IEEE 802.11 standardını yayımlamıştır. Bu standarda göre 2.4 GHZ frekans bandında çalışmaktaydı. Aynı zamanda, FHSS(Frenquency Hopping Spread Spectrum) ve DSSS (Direct Sequence Spread) kullanmaktaydı ve 2 Mbps’e kadar data iletişimi gerçekleştirebilmekteydi **(Agilent Technologies, 2005).** 802.11 standardındaki temel amaç mevcut kablolu LAN’ların kablosuz hale gelmesini sağlamak ve kablolu sistemlerle mobil sistemleri uyumlu olarak çalıştırmaktır. Zaman içerisinde IEEE tarafından yayımlanan standardın başarılı olması ile 802.11x ile yeni standartlar yayımlanmıştır.

802.11 cihazları ISM bantlarını kullanmaktadır. İlk ISM bandı 900 MHz’di. Buna karşın ilk defa US’de kullanıldı. 2.4 GHz ISM band 802.11b ve 802.11g aygıtlarında kullanıldı. US’de 11 kanal tanımlamasına karşın, Avrupa 13 kanal tanımladı. Her bir kanalın bant genişliği her bir bandın merkezleri arasından 5 MHz olarak dağılmış 22 MHz’lik dağılıma sahiptir. Çizelge 5.1.’de kanallara ait frekanslar ve şekil 5.3.’de 2.4 GHz’de 802.11 kanal tahsisi görülmektedir (Holt ve Huang, 2010).

1

2

3

4

5

6

7

8

9

10

11

12

13

22 MHz

Şekil 5.3. 2.4 GHz bandda 802.11 kanal tahsisi (Holt ve Huang, 2010)

Çizelge 5.1. 2.4 GHz bandda kanal tahsisi (Holt ve Huang, 2010)

| **Kanal** | **Frekans** | |
| --- | --- | --- |
| **Düşük** | **Yüksek** |
| 1 | 2.401 | 2.423 |
| 2 | 2.406 | 2.428 |
| 3 | 2.411 | 2.433 |
| 4 | 2.416 | 2.438 |
| 5 | 2.421 | 2.433 |
| 6 | 2.426 | 2.448 |
| 7 | 2.431 | 2.453 |
| 8 | 2.436 | 2.458 |
| 9 | 2.441 | 2.463 |
| 10 | 2.446 | 2.468 |
| 11 | 2.451 | 2.473 |
| 12 | 2.456 | 2.478 |
| 13 | 2.461 | 2.483 |

Çizelge 5.2.’de 802.11x standartlarına ait teknik özellikler detaylandırılmıştır.

**Çizelge 5.2.** 802.11 x standardının sınırları ve bazı özellikleri (1Holt ve Huang, 2010, 2CISCO Technical Presentation, 2007, 3Agilent Technologies, 2005, 4Redpine Signals, 2011)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Standart Adı** | **Frekans Bandı** | **Modülasyon Tekniği** | **Güvenlik** | **Veri Hızı** | **Kapsama Alanı**  **(Yaklaşık)** | **Kabul Ediliş** |
| IEEE 802.11 | 2,4 GHz | FHSS veya  DSSS | WEP veya  WPA | 2 Mbps | - | 1999(ISO/IEC) |
| IEEE 802.11a | 5 GHz | OFDM | WEP veya WPA | 54 Mbps | A:~100m K:~13m | 16/09/1999 |
| IEEE 802.11b | 2,4 GHz | DSSS | WEP veya WPA | 11 Mbps | A:~110m K:~35m | 16/09/1999 |
| IEEE 802.11g | 2,4 GHz | DSSS veya OFDM | WEP veya WPA | 54 Mbps | A:~110m K:~35m | 12/06/2003 |
| IEEE 802.11n | 2.4/5 GHz | MIMO-OFDM | WPA veya WPA2 | 300 Mbps | A:~250m K:~70m | 30/09/2009 |

A: Açık alan, K:Bina İçi

**DSSS (Direct Sequence Spread Spectrum)** İletilen veriye, rastlantısal olarak belirlenmiş bir bit dizisi ile XOR(Özel-veya) işlemi uygulanır. DSSS tekniği 802.11b standardında kullanılan kodlama ve modülasyon yöntemidir. 802.11b standardında maksimum 11 Mbps veri oranında kodlama yapabilmektedir.

**FHSS (Frequency Hopping Spread Spectrum),** frekans atlamalı dağılmış spektrum olarak Türkçeye çevrilebilmektedir. 802.11 standardında FHSS ve DSSS teknikleri kullanılabilmektedir. Fakat, dezavantajlarından dolayı sonraki standartlarda tercih edilmemiştir. FHSS yayılmış kod modülasyonu için frekans kaydırmalı anahtar (FSK) kullanmaktadır. Aygıtlar kısa bir periyot için(bekleme süresi olarak bilinen) ortak bir frekans üzerinde iletmekte/almaktadırlar. Aygıtlar (iletim ve alımda) pseudo-random dizi içinde kanaldan kanala atlamaktadır. Farklı alıcı/iletici çiftleri aynı kanalda çarpışmaları en aza indirgemek için farklı bir pseudo-random dizi kullanmaktadır. . (Holt ve Huang, 2010)

**OFDM (Orthogonal Frequency Division Multiplexing)** Dikey frekans bölümleme çoğullama olarak ifade edilebilmektedir. Kanal sayısının fazla olduğu kablosuz ağ kurulumunda önemli bir tekniktir. Çünkü her bir kanal aslında bağımsız bir iletişim ortamıdır. OFDM’de 20 MHz’lik 8 tane çakışmayan kanal tanımlanmıştır. Kanalların her biri 52 alt taşıyıcıya bölünmüştür. Böylece belirli bir zamanda yapılabilecek bağımsız aktarım sayısı artırılmıştır. 54 Mpbs hıza ulaşmak için 64 QAM adlı mekanizma kullanılmaktadır.

**MIMO (Multiplie Input Multiplie Output)** Kablosuz haberleşme sistemlerinde gönderici ve alıcıda çoklu antenler sayesinde yüksek data hızlarına ulaşılabilmektedir. MIMO sistemleri çoklu antenleri ve iletici/alıcıda RF dizisini gerektirmektedir. Vericide anten/RF dizilerinin sayısı (nT) alıcıda (nR) aynı sayıda olmasını gerektirmemektedir. MIMO teknolojisi OFDM sistemlerinin çoklu dar bantları içinde iletilen sinyalleriyle uyumludur. MIMO-OFDM, yüksek veri oranları arayışı için araştırmacılar için önemli bir ilgi alanıdır. (Holt ve Huang, 2010)

**IEEE 802.11b Standardı**

802.11b, 802.11a ile aynı tarihte çıkmıştır. DSSS modülasyon tekniğini kullanmaktadır. 2.4 Ghz bandında 2400-2483.5 Mhz aralığında 11 Mbps’a kadar veri iletişim hızlarına sahip olabilmektedir. Dizüstü ve masaüstü bilgisayarlar da yaygın bir şekilde kullanılmıştır. Ancak zaman içerisinde diğer standartların üstün özellikleri kullanım oranlarını düşürmüştür. 802.11b standardının en büyük problemlerinden biriside enterferasyon olasılığıdır. Bu durum veri iletişim hızını düşürmekte yâda kopmalara neden olabilmektedir.

* + 1. **IEEE 802.11a Standardı**

OFDM modülasyon tekniği kullanarak 5 GHz frekans bandında 54 Mbps veri iletişim hızına sahiptir. Bu teknoloji 802.11b’ye göre daha üstün bir standarttır. 802.11b’de 11Mbps olan veri iletişim hızı 802.11a’da 54 Mbps’e çıkmıştır. Hızın artması ise videolarda kesintisiz görüntü elde etmede önemli olduğundan 802.11a standardında daha etkili sonuçlar elde edilebilmiştir. Radyo frekansları vericiden alıcıya doğru giderken OFDM tekniği sinyal iletiminde daha verimli sonuçlar doğurmaktadır. Çünkü OFDM sinyal yansımalarından daha az etkilenmektedir. 802.11b’ye göre kapasitesi daha yüksektir. 5 Ghz bandında enterferans yapmayan 12 kanal WLAN sistemleri için ayrılmıştır. 2,4 Ghz bandında ise sadece 3 kanal bulunmaktadır.

802.11a’da veri iletişim hızı 54 Mbps olduğu için 802.11b’ye göre 5 kat daha hızlıdır. 802.11b, Orthogonal Frequency Division Multiplexing (OFDM) modülasyon tekniğini kullanmakta ve 5 Ghz frekans bandında çalışmaktadır. Bu durum enterferans riskini 802.11b’ye göre düşürmektedir.

### 5.1.3. IEEE 802.11g Standardı

802.11b gibi 2.4 GHz bandında çalışmaktadır. Bu standart toplam 54 Mbps bant genişliği sunar. OFDM modülasyonunu kullandığından yüksek hızda çalışmaktadır. Bu modülasyon 802.11a standardında da kullanılmaktadır. 802.11g'nin dezavantajları 802.11b benzerleri ile aynı olup üst üste binmeyen sadece üç kanal kullanılması ayrıca yüksek frekans yayılımı yapan mikrodalga fırın gibi sistemlerden etkilenmesidir.

### 5.1.4. IEEE 802.11n Standardı

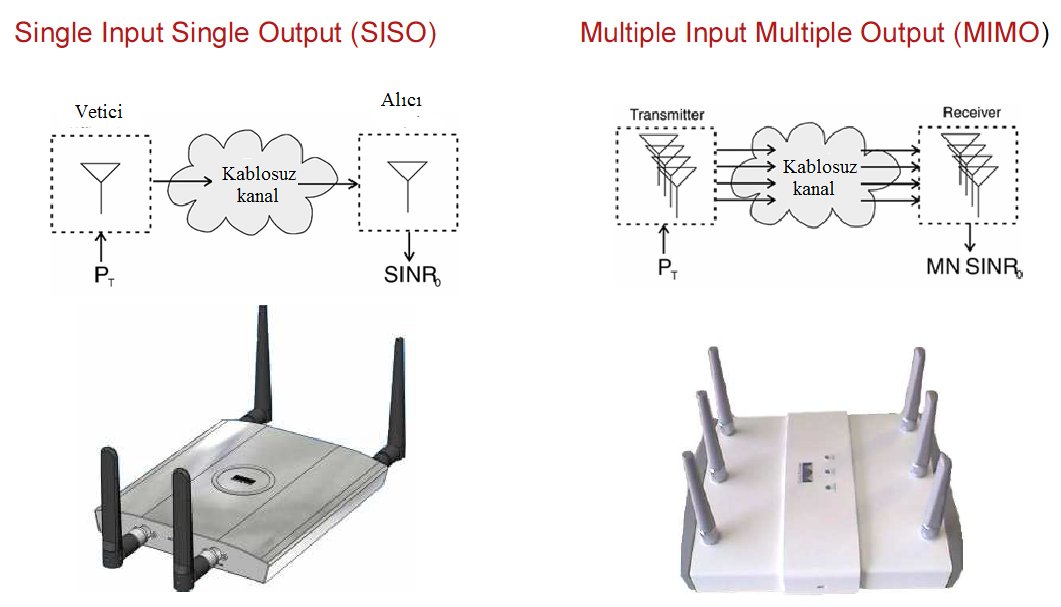
Yüksek bant genişlikli data, ses ve video uygulamaları için çok iyi sonuç veren bir standarttır.

* 5 kat daha yüksek veri hızı
* Daha güvenilir ve tahmin edilebilir yorumlama

802.11 a/b/g alıcılarıyla uygunluk sağlayabilmektedir.

|  |  |  |
| --- | --- | --- |
| **Temel olarak 802.11n Bileşenleri (CISCO Technical Presentation, 2007)** | | |
| * **Multiplie Input Multiplie Output (MIMO)**   Maksimum oranlı birleştirme (MRC)  Radyo sinyalini şekillendirme  Uzaysal çoklama | * **40 MHz kanallar**   İki bitişik 20 MHz kanal tekil bir 40 MHz kanal oluşturmak için birleştirilmektedir. | * **Geliştirilmiş MAC verimi**   Tekil bir iletim içinde, paket toplama- paketleri birleştirme .  Blok tanıma |

Şekil 5.4.’de SISO ve MIMO türü haberleşme modülasyon türleri farklılığı ortaya koyulmuştur. SISO’ta tekil gelen tekil çıkar sistemiyle çalışmaktadır. MIMO’da gelen sinyallerinin hepsininde işleme tabi tutulacağı temsili olarak gösterilmiştir. (CISCO Technical Presentation, 2007)



Şekil 5.4. SISO ve MIMO iletişim

**Maksimum birleştirme oranı**

* Alıcı tarafından yerine getirilmektedir
* Çoklu alıcı sinyallerini birleştirir
* Alıcı hassasiyetinin arttırılmıştır
* MIMO’suz ve MIMO kullanıcıları ile çalışır

**İletilen sinyali biçimlendirme**

* Verici tarafından gerçekleştirilmektedir
* Sağlanan sinyal fazında alınır
* Duyarlılık artmaktadır
* MIMO ve MIMOsuz kullanıcılar ile çalışmaktadır

**Uzaysal Çoklama**

* Verici ve alıcı ortaktır
* Çoklu antenler txmt aynı kanalları birleştirir
* Duyarlılık artmaktadır
* MIMO gerekmektedir



Mesaj

Mesaj

Mesaj

Mesaj

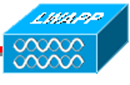
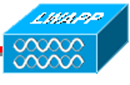
Mesaj

Mesaj



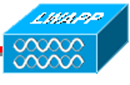
Mes

aj



Mesaj

Mesaj



Mesaj

Şekil 5.5. MIMO Sinyal İletimi (CISCO Technical Presentation, 2007)

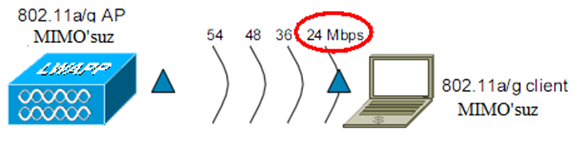
1. **MIMO Tüm İstemciler İçin PHY Data Oranları**

Maksimum Oranda

Birleştirme (MRC)

Işın Birleştirme

Uzaysal Çoklama

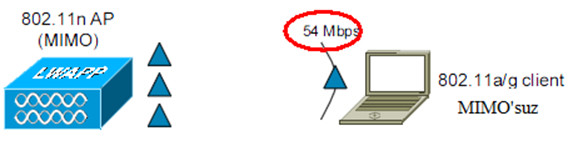


Maksimum Oranda

Birleştirme (MRC)

Işın Birleştirme

Uzaysal Çoklama

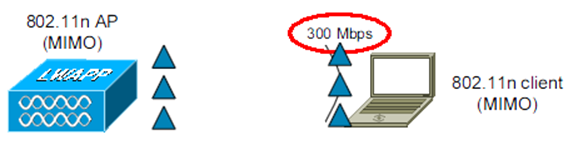


Maksimum Oranda

Birleştirme (MRC)

Işın Birleştirme

Uzaysal Çoklama



Şekil 5.6. MIMO Seçenekleriyle iletim hız değişimi(CISCO Technical Presentation, 2007)

1. **40 MHz Kanallar ve Paket Birleştirme**

***40-MHz Kanallar:*** 802.11n 20 MHz ve 40 MHz genişlikte kanalları desteklemektedir. Geniş kanallar, AP başına daha fazla BW anlamına gelmektedir Bu durum yolun tek şeritten iki şeride çıkmasına da benzetilebilir.



40 MHz

20 MHz

20 MHz

802.11n

Üst başlığı

Data Ünitesi

Paket

802.11n

Üst başlığı

Data Ünitesi

Paket

802.11n

Üst başlığı

Data Ünitesi

Paket

802.11n

Üst başlığı

Data Ünitesi

Paket

Paket

Paket

Paket birleşimi olmadan

Paket birleşimli

Şekil 5.7. 802.11n’de paket birleştirme(CISCO Technical Presentation, 2007)

***Paket birleştirme:*** Başlangıçta ayrık halde olan verilerin birleştirilme işlemi gerçekleşecektir. Bu işlem paketlerin tek bir MAC başlığında saklamasıyla gerçekleştirilmektedir.

İlk 20 MHz kanal

İkinci 20 MHz kanal

20 MHz ve 40 MHz ikiside, tüm kontrol ve yönetim çerçevelerinde ilk kanalda iletilmektedir

Bu hücrede trafik 20 MHz’dir.

20 MHz kanalda kesişen hücrelerin içinde trafik

20 MHz 🡪 40 MHz’ye Geçiş

Bu hücrede Trafik 40 MHz’dir.

40 MHz 🡪 20 MHz’ye Geçiş

Bu hücrede trafik 20 MHz’dir.

20 MHz kanalda kesişen hücrelerin içinde trafik

Frekans.

20 MHz işlem

40 MHz işlem

20 MHz işlem

Şekil 5.8.. 802.11n’de 20/40 MHz operasyon (Marsic, 2010)

802.11n standardında iki bitişik 20 MHz kanal tekil bir 40 MHz kanal oluşturmak için birleştirilmektedir. Şekil 5.8.’de bu yapı anlatılmaktadır. Görüldüğü gibi frekans 20 MHz’de ise üst kısım devrede, 40 MHz’ye geçildiğinde ise iki frekans bölgesi birleştirilerek 40 MHz bandına geçilecektir.

FC

2

D/I

2

Adress-1

6

Adress-2

Adress-3

SC

Adress-4

QC

HT CONTROL

DATA

FCS

6

6

2

6

2

4

0’dan 7955’e

4

DATA

FCS

MSDU

MAC

HEADER

PHY

HEADER

PHY

PREAMBLE

PSDU=MPDUMSDU

(a)802.11 için çerçeve yapısı

(b) 802.11 n link katmanı çerçeve formatı

PPDU= PLCP protocol data unit

PSDU= PLCP service data unit

MPDU=MAC protocol data unit

MSDU= MAC service data unit

PLCP= physical (PHY) layer converange procedure

MAC=medium Access control

PPDU

Şekil 5.9. Çerçeve formatları (Marsic, 2010)

Şekil 5.9.’da 802.11 ve 802.11n için link katmanı çerçeve formatları verilmiştir. 802.11’in link katmanı ile karşılaştırıldığında ***HT Control*** alanının eklendiği ve çerçeve data kalıbının değiştiği göze çarpmaktadır. Çerçeve yapısının maksimum uzunluğu 7955 byte’dır ve tüm tüm 802.11n çerçeve uzunluğu 8Kbyte’dır.

DIFS

Busy

Yaklaşık 64 Kbyte’a (toplanmış data yükü)

FCS

MAC header

PHY header

PHY preamble

0’dan 2312 byte’a(Data Yükü)

Overhead

ACK

PHY header

PHY preamble

FCS

MAC header

FCS

MAC header

PHY header

PHY preamble

Busy

1. IEEE 802.11 için link katmanı
2. IEEE 802.11n çerçeve kümesi

Overhead

SIFS

Şekil 5.10. Çerçeve Yapıları(Marsic, 2010)

Çerçeve yapıları karşılaştırıldığında 802.11n’de yaklaşık 64 kByte’a çıkan veri miktarı dikkati çekmektedir. Bu faktör kendisini saniyede iletilen veri miktarının yüksekliği ile göstermektedir.

1. **MAC Servis Data Ünitesi (MAC Service Data Units(MSDUs)) Kümesi**

MSDU kümesinin çerçeve formatları aslında çoğu mobil Access point’de kullanılmaktadır ve çoğu mobil alıcı protokol yığınları doğal çerçeve formatı olarak Ethernet kullanmaktadır. MSDU, 802.11n çerçevesi içinde paketler ve tekil bir hedefe ulaştırmak için Ethernet çerçevesinde toplar. Bu çok verimlidir çünkü Ethernet başlıkları 802.11 başlığından çok daha kısadır. Bu nedenle MSDU MPDU’dan daha verimlidir. MSDU kümesi A-MSDU ‘ya bağlanmış birkaç MSDUs’ya izin vermektedir. (Marsic, 2010)

Kaynak mobil bir aygıt olduğunda, toplanmış çerçeve Access pointe gönderilir, burada Ethernet çerçeveleri bileşenleri onların nihai hedeflerine sevk edilmektedir.

1. **MAC Protokol Data Üniteleri (MAC Protokol Data Units(MPDUs))**

MPDU kümesi de tekil bir alıcıya iletmek için Ethernet çerçeveleri ekler, fakat 802.11n çerçeveleri içinde verileri dönüştürür. Normalde bu MSDU kümesinden daha az verimlidir, ama yüksek veri oranlarıyla daha verimli olabilmektedir, çünkü tasarlanan mekanizma blok onay çağırma özelliğine sahiptir.

RIFS

DIFS

PHY preamble

Subframe 1

Busy

PHY header

802.11n

MAC header

Subframe N

FCS

ACK

SIFS

…..

Ethernet header

Data

Padding

DIFS

PHY preamble

Subframe 1

Busy

PHY header

Subframe N

Block ACK

RIFS

802.11n MAC header

Data

FCS

…..

SIFS

Padding

MPDU Delimiter

MPDU

A-MPDU subframe

A-MSDU = Ethernet çerçevesi kümesi (=PSDU 8 KB’a kadar)

MSDU subframe=Ethernet çerçevesi

A-MPDU = 802.11n çerçeve kümesi (=PSDU 64 KB’a kadar)

1. MPDU kümesi
2. MSDU kümesi

Şekil 5.11. 802.11n Çerçeve sınıfı çeşitleri(Marsic, 2010)

MPDU kümesi tekil bir PPDU(PHY layer protocol data unit) içine birkaç MPDUs kümesi dahile edebilir. Şekil 5.11.b.’de MPDU’nun çerçeve yapısı görülmektedir. Şekilde görüldüğü gibi A-MPDU, MPDU sınırlayıcıların (delimiters) sayısı kadardır. Bunun haricinde bir A-MPDU içinde A-MPDU alt çerçevesinde son sırada bulunan padding byte, alıcının tarifini yapmayı kolaylaştıcı 4 byte uzunluğuna sahip olarak eklenmektedir.

ACK bloğu kurulumu

Data ve ACK bloğu iletişimi

Gönderici

Alıcı

ACK

AddBA isteği

AddBA yanıt

ACK

Gönderici

Alıcı

MPDU bilgisi

MPDU bilgisi

MPDU bilgisi

BlockAckReq(BAR)

ACK Bloğu

DelBA İsteği

ACK

Ack Bloğu Teardown

Şekil 5.12. Başlama, kullanım ve 802.11n blok onayın iptali (Marsic, 2010)

Şekil 5.12’de 802.11n’de MPDU bilgisinin iletilmesi için gerekli işlem adımları grafiksel olarak gösterilmektedir. İlk aşamada ACK bloğunun kurulumu, ikinci aşamada Data ve ACK bloğu iletişimi ve son aşama ise Teardown ile kesme işlemi gerçekleştirilmesidir.

* 1. **802.11 Kablosuz Ağlarında Güvenlik Protokolü**

802.11 standardına sahip kablosuz ağların kullanımları giderek yaygınlaşmaktadır. Bununla birlikte bu ağları kullanan sistemlerde zaman içerisinde güvenlik problemleri ortaya çıkmaya başlamıştır. Bunun için güvenlik konusunda farklı şifreleme algoritmaları geliştirilmiş olup çeşitli kablosuz ağ uygulamalarında kullanılmaya başlanmıştır. Kablosuz ağ kullanan sistemlerde güvenlik önlemleri konusunda, ***IEEE, 802.11i*** standardı geliştirilmiş. Bu standart çerçevesinde çeşitli şifreleme algoritmaları geliştirilmiş, yetersiz algoritmaların yerini daha kuvvetli algoritmalar almıştır. Böylece kablosuz ağlarda güvenli bir ortam sağlamaya çalışılmaktadır. Bu güvenlik politikaları, WEP, WPA, WPA2, 802.1X kimlik doğrulaması olmak üzeredir. Kablosuz güvenlik protokolleri Data Link katmanında bulunmaktadır.

FHSS

802.11 2M bps

DSSS

802.11 2 M bps

HR/DSSS

802.11b

HR/DSSS 802.11g

OFDM 802.11g

54 Mbps

MIMO 802.11n

300 Mbps

OFDM 802.11a

54 Mbps

2.4 GHz ISM Band

5 GHz ISM

**WEP**

**WPA**

**WPA2**

IEEE 802.11 Media Access Sub-Layer

IEEE 802.1 Bridging

IEEE 802.2 Lojik Bağlantı Kontrolü

IP/ARP Encapsulation

(RFC 1024)

IEEE 802.11H Bridge Tunneling

TCP/IP

IPX

Apple/Talk

Üst Katman

Data Link Katmanı

Fiziksel Katman

Şekil 5.13. Güvenlik protokollerinin OSI modelindeki yeri (Lashkari, Danesh, vd., 2009)

* + 1. **WEP (Wired Equivalent Privacy)**

WEP, 802.11 kablosuz ağ güvenlik standartlarındandır. WEP’in temel görevi radyo dalgaları üzerinden bilgilerin kurulan algoritma ile şifrelenmesini sağlamaktır. WEP, eylül 1999’da 802.11 standardının bir parçası olarak onaylanmıştır. WEP’te kullanılan anahtar veri uzunluğu 40 yada 104 bittir.

Şekil 5.14.’de örnek bir WEP şifreleyicisi ve çözücüsü görülmektedir. Burada, 24 bitlik başlangıç vektörü (IV), 40 bitlik paylaşılan anahtara eklenir. Bu anahtar bilgisi ile RC4 algoritması kullanılarak şifrelenecek veriyle aynı boyutta akış şifresi elde edilmektedir. IV vektörünün değişmesi ile her seferinde farklı akış şifreleri elde edilmektedir. Elde edilen akış şifresi ile Paket ex-or işleminden geçirilerek şifreli metin hazırlanmış olur. Böylece gönderilecek veri hazırlanmış olur.

Şifre çözmede ise alıcı taraf IV yi çerçeve den okur ve paylaşılan anahtar AP’ dede olduğundan bu iki bilgiyi işleme tabi tutar ve akış şifresini elde edebilir. Şifreleme işlemlerini ters sıra ile gerçekleştirerek açık veriyi elde eder.

Yük

CRC

CRC Algoritma Üreteci

Yük

Paylaşılan anahtar

IV Jenerasyon Algoritma

Sıralanmış IV ve Key

Paket Başına Anahtar

RC4 Algoritması

RC4 Algoritması

Paket Başına Anahtar

Sıralanmış IV ve Key

Paylaşılan anahtar

Paket

Yük

CRC

Anahtar akışı

Düz giriş

Düz çıkış

Şifreli

Anahtar akışı

24 bitlik IV

Yüklü bitler anahtar akışıyla XOR işlemine tabi tutulur

Radyo vericisi

AP

Paket

Şekil 5.14. WPA ile text’in şifrelenmesi (Scarfone, Dicoi, 2008)

WEP’te kullanılan RC4 şifreleme algoritmasındaki zayıflıklar, anahtar yönetim mekanizmasının olmaması ve 24-bit initialization Vector(IV) kullanımının tekrarlanan şifreleme dizilerinde kullanılması yeterince gizlilik sağlayamamaktadır. Bu ve benzeri açıklardan dolayı WEP artık önerilmemektedir. Çünkü WEP güvenliğini kırmak göreli olarak daha kolaydır. (www.microsoft.com)

* + 1. **Wi-Fi Korumalı Erişim (WPA)**

WEP standartlarından RC4 algoritmasında bulunan güvenlik açıklarını kapatmak için Wi-Fi Alliance WPA’yı oluşturmuştur. WPA bilgiyi şifreler ve ayrıca ağ güvenliği anahtarının değiştirilip değiştirilmediğini de denetler. Ayrıca WPA, yalnızca yetkili kişilerin ağa erişebilmesini sağlamaya yardımcı olmak için kullanıcıların kimliğini de doğrular. WPA, TKIP (Temporal Key Integrity Protocol- Tekli şifrelemede Geçici Anahtar Bütünlüğü Protokolü) ‘i desteklemektedir. TKIP, kablosuz aygıtların şifreleme işlemlerini daha güçlü bir şekilde gerçekleştirmektedir. TKIP şifreleme anahtarları belirlendikten sonra, güvenlik yapılandırmasının doğrulanması, şifreleme anahtarının eşzamanlı olarak değiştirilmesi özellikleri ile WEP’e göre üstünlük sağlamaktadır. WPA’da Anahtar uzunluğu olarak 128 bit kullanılır. WPA’ da daha güçlü olan MIC(Message Integraty Code) mekanizması ile sağlanır. WPA’da anahtar yönetimi için 802.1x kullanılır. Kimlik doğrulama için WPA, 802.1x EAP ile güçlü bir yöntem kullanılmıştır.

Evre-1 Anahtar Karıştırıcı

Evre-2 Anahtar Karıştırıcı

WEP

Fregmantasyon

Michael

Geçici

Anahtar

Gönderici Adresi

Sıra Sayıcı

MIC Anahtarı

Frame verisi: yük, kaynak, hedef

Açık metin çerçevesi

WEP IV

WEP Gizli

Anahtar

İletim İçin Şifrelenmiş ve Kimliği Doğrulanmış Çerçeveler

Şekil 5.15. TKIP’de veri şifreleme (Mertkan ve Buluş, 2009)

*WEP IV: Wired Equivalent Privacy Inıtialization Vector,*

*MIC– Message Integrity Check*

Şekil 5.15.’de TKIP’te veri şifreleme blok diyagramlarla anlatılmaktadır.

TKIP’in temel özellikleri:

* TKIP’te her çerçeve için bir RC4 anahtarı üretmektedir. Her bir anahtarın üretildiği sürece, anahtar karıştırma denmektedir,
* Çerçevelerin sıra sayaçları vardır,
* TKIP, Michael denilen hashing algoritması kullanmaktadır,
* Çerçevelerin çalınmasına karşı güvenlik için geliştirilmiş önlemlerde içermektedir,
* TKIP’te anahtarlar güçlüdür ve IV 48 bite çıkarılmıştır,
* IV(Initialization Vector) hem paketlere sıra numarası vermek, hem de her paket için tek kullanımlık anahtar üretmede de kullanılmaktadır,
* Anahtar uzunluğu 128 bite çıkarılmıştır
* Bir MIC anahtarı michael’le, yapısal içeriğini korumaktadır. Kurulmuş olan bu sistemle, MIC anahtarı ile AP’den istemci arasındaki MIC anahtarından farklıdır. Verici adresi, TKIP’e bir giriş rolü oynar. Verici adresi çerçeveden sağlanmaktadır. Şekil 5.15’de görülen giriş sinyalleri ile devrede işlenir ve WEP bloğundan geçirilerek güçlü bir şifreleme sağlanır.(Mertkan ve Buluş, 2009)

Bilgi çerçeve içinde bulunduğundan, şekil 5.15’de sağ üst köşeden girmektedir.

İki tür WPA kimlik doğrulaması vardır: WPA ve WPA2. WPA tüm kablosuz ağ bağdaştırıcıları ile çalışmak üzere tasarlanmıştır, ancak eski yönlendiriciler veya erişim noktalarıyla çalışmayabilir.

* + 1. **802.1x**

802.1X kimlik doğrulaması 802.11 kablosuz ağlarının ve kablolu Ethernet ağlarının güvenliğini artırmaya yardımcı olabilir. 802.1X kullanıcıları doğrulamak ve ağ erişimi sağlamak için bir kimlik doğrulama sunucusu kullanır. 802.1X, kablosuz ağlarda, Kabloluya Eşdeğer Gizlilik (WEP) veya Wi-Fi Korumalı Erişim (WPA) anahtarlarıyla birlikte çalışabilir. Bu kimlik doğrulama türü genellikle çalışma alanı ağına bağlanırken kullanılır (www.microsoft.com)

* + 1. **WPA-2 Şifrelemesi (IEEE 802.11i)**

IEEE 802i güvenlik standardı, WEP’in zayıf noktalarına önlem olarak ortadan kaldırmaya yöneliktir. AES (Advanced Encryption Standard) şifreleme algoritmasının Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) modunda şifreleme ve kimlik doğrulama/yetkilendirme için 802.1x’in kullanımını önermektedir. AES şifreleme algoritması RC4 algoritmasıyla kıyaslandığından çok daha güvenlidir.

WPA2, WPA'ya göre daha güvenlidir, ancak bazı eski ağ bağdaştırıcılarıyla çalışmaz. Bu, WPA-Kuruluş veya WPA2-Kuruluş olarak adlandırılır. Ayrıca, her kullanıcıya aynı parolanın verildiği önceden paylaştırılan anahtar (PSK) modunda da kullanılabilir. Bu, WPA-Kişisel veya WPA2-Kişisel olarak adlandırılır

* 1. **Diğer Kablosuz Ağlar**

Bu bölümde WLAN ağların dışında kalan bazı kablosuz ağ türlerinin özellikleri incelenecektir.

### 5.3.1. Zigbee

IEEE 802.15.4 standardına bağlı olarak çalışan bir Kablosuz algılayıcı ağı (Wireless Sensor Network, WSN) teknolojisi’dir. Zigbee bu standart tarafından belirlenmiş olan özellikleri taşımaktadır.

PAN’lar için geçtiğimiz yıllara kadar iki temel standart bulunmaktaydı. Bunlar: Bluetooth ve WiFi olmak üzereydi. Endüstride de temel olarak kablosuz iletişim sırasında daha az karmaşıklık ve birçok durumda pil ömrünün neden olduğu sorunlara çözüm getirmesi özellikleri ile öne çıkmaktadır. (Lee, Su, vd., 2007) Zaman içerisinde IEEE 802.15.4-2003 temel alınarak ve daha sonra ZigBee Alliance’ın aralık 2004’te devreye girmesiyle PAN ağlar içerisine girmiştir.

Çizelge 5.1 . Zigbee Karakteristik değerleri (Qu, Wang vd., 2010)

|  |  |
| --- | --- |
| **Karakteristik** | **ZigBee** |
| IEEE tipi | 802.15.4 |
| İşlem Frekansı | 868 MHz, 902- 928 MHz, 2.4 GHz- ISM |
| Data Oranı | 20 -250 kb/s |
| Nominal TX gücü | -25-0 dBm |
| Nominal aralık | 10-75 m |
| Hücre düğümleri’nin maksimum sayısı | 65000 |

ZigBee, PAN’da ki radyo iletişimi ile ara bağlantısı sağlanan cihazları ve temel alınan protokolü tanımlamaktadır. ZigBee CSMA/CA ortam erişimi mekanizmasını kullanmaktadır. (Callaway, Gorday vd., 2002) Çalışma menzili, 10 ile 75 metre arasında değişmektedir. (Qu, Wang vd., 2010)

ZigBee teknolojisi temel olarak dört temel topolojiyi kullanır: Peer-to to-Peer (P2P), Star, Mesh ve Cluster Tree olmak üzeredir. Bunlar aşağıdaki şekilde de görülebilmektedir.



Şekil 5.16. Zigbee teknolojisinde kullanılan ağ türleri

ZigBee teknolojisi geniş çaplı ağların daha düşük maliyetle kurulmasını sağlayabildiği gibi kontrol ağları uygulamalarında da kullanılabilmektedir. Zigbee teknolojisi mesh ağı teknolojisini de desteklemektedir.

İlk zamanlar askeri amaçla kullanılan kablosuz algılayıcılar; zamanla maliyetlerinin düşmesi ile birlikte çok yaygın olarak kullanılmaya başlamıştır. Algılayıcı ağlar temel olarak nem sıcaklık basınç, ışık ve hareketlilik gibi durumsal değişiklikleri takip etmek için değişik yapılara sahip olabilmektedir. Savunma sanayinde uçaklarda mevcut donanım bilgisine ulaşmak, düşman askerlerini izlemek, çevresel değişiklikleri izlemek gibi yerlerde kullanılabilmektedir. Bunlara ek olarak, bina içinde kablosuz haberleşmeyi gerçekleştirmek için kullanılabilir bir teknolojidir.

* + 1. **Bluetooth**

Bluetooth, kablo bağlantısı ile veri iletişimini ortadan kaldıran kısa mesafe Radyo Frekansı (RF) teknolojisinin adıdır. (Lee, Su, vd., 2007) Kablosuz kişisel alan ağları (WPAN) içinde çalışmakta olup IEEE tarafından belirlenmiş olan 802.15.1 standardını kullanmaktadırlar.

Bluetooth sisteminin çalışması kumandalarda kullanılan sistem infra-red (IRDA) (kızıl ötesi olarak da bilinmektedir) teknolojisine dayanmaktadır. Bluetooth teknolojisi sayesinde Mouse, klavye, printer gibi cihazlar kablosuz şekilde bilgi transferini gerçekleştirebilmektedirler. 2.4 gigahertz (GHz)’den 2.485 GHz’e kadar giden aralıkta lisanssız olarak kullanılmaktadır. Bluetooth, modülasyon olarak FHSS(frequency hopping spread spectrum)’yi kullanmaktadır. FHSS ile interferens ve iletim hataları azalmakta ve iletim güvenliği artmaktadır. FHSS teknolojisiyle, Bluetooth cihazları arasında iletişim data/ses linklerinde saniyede 1600 kez ve sayfa taramalarında saniyede 3200 kez değişen frekans aracılığıyla, 79 farklı radyo kanalı kullanmaktadır.( Scarfone ve Padgette, 2008)

Çizelge 5.2. Bluetooth aygıt sınıflarına göre güç gereksinimleri.( Scarfone ve Padgette, 2008)

|  |  |  |  |
| --- | --- | --- | --- |
| Tip | Güç | Güç Seviyesi | Kapsama Alan Sınırları |
| Sınıf 1 | Yüksek | 100 mW (20 dBm) | 91 metreye kadar |
| Sınıf 2 | Orta | 2.5 mW (4 dBm) | 9 metreye kadar |
| Sınıf 3 | Düşük | 1 mW (0 dBm) | 1 metreye kadar |

Bluetooth versiyon 1.1 ve 1.2’de 1 megabite kadar aktarım hızı belirtilmekte iletilen veri (throughput) saniyede yaklaşık 720 kilobit’e ulaşmaktadır. Bluetooth versiyon 2.0 + Enhanced Data Rate (EDR) ve 2.1 + EDR veri oranı 3 Mbps belirlenmiş olup iletilen veri yaklaşık (throughput) 2.1 Mbps ‘dir.

Çizelge 5.3. Bluetooth karakteristikleri (Qu, Wang vd., 2010)

|  |  |
| --- | --- |
| **Karakteristik** | **Bluetooth** |
| IEEE tipi | 802.15.1 |
| İşlem Frekansı | 2.4 GHz ISM |
| Data Oranı | 1 Mb/s |
| Nominal TX gücü | 1. 10 dBm |
| Nominal aralık | 10-100 m |
| Hücre düğümleri’nin maksimum sayısı | 8 |

Bluetooth iki bağlantı topolojisine sahiptir: piconet ve scatternet.

1. **Piconet**

Bluetooth ağları sekiz cihaza kadar birlikte “master- slave” durumunda bir ağ oluşturabilirler ki buna “pikonet” (piconet) denilmektedir. Birbirlerinin kapsama alanı içerisinde bulunan Bluetooth birimleri noktadan noktaya ya da noktadan çok noktaya bağlantı kurabilirler. İki veya daha fazla bluetooh birimi birbiriyle bağlantı kurduğunda bunlar bir şebeke oluştururlar ve Bluetooth standartlarında bu şebekeye ‘piconet’ adı verilir. Pikonetler yedi aktif slave durumunda ve 255 aktif olmayan cihaza bağlanabilmektedir. (Scarfone ve Padgette, 2008) Piconet, master - slave ilişkisiyle kablosuz ağ zincirini belirlenmiş olan kurallar dahilinde oluşturabilmektedir.

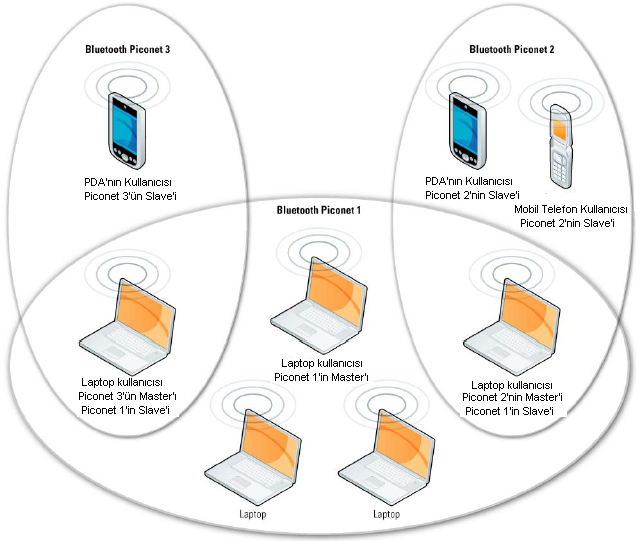
Bir piconet, bir veya daha fazla bağlı olan Bluetooth ile WPAN ağı oluşturmaktadırlar (Lee, Su, vd., 2007). Piconet bağlantısı şekil 5.17.‘de verilmiştir. Bluetooth teknolojisini kullanan cihazlar, ad-hoc biçimiyle bağlantı kurmaktadırlar. Bir frekans atlamalı kanal, master olarak her bir piconetin adresi üzerinden tanımlıdır.



Şekil 5.17. Piconet Bağlantı Sistemi

1. **Scatternet**

Birden fazla Piconet’in birbirine bağlanmasıyla oluşan şebeke yapısına Scatternet adı verilir. Scatternet yapısı kullanılarak ağ içerisindeki birim sayısı attırılabilir ve daha geniş bir kapsama alanı elde edilebilir.



Şekil 5.18. Scatternet Bağlantı Sistemi. (Scarfone ve Padgette, 2008)

* + 1. **UWB**

UWB teknolojisi kapalı ortamlarda, kısa mesafeli yüksek hızlı iletişimle dikkatleri çekmektedir. UWB’nin en dikkat çekici özelliklerinden birisi de bant genişliğinin, ev ağı içinde ses ve video sunumlarında 110Mbps(480 Mbps’e kadar)’in üzerinde olmasıdır (Lee, Su, vd., 2007). Birleşik devletler ve Federal iletişim komisyonu (FCC) 2002’de UWB için frekans tahsisi yapmış, Elektronik iletişimleri komitesi (ECC TG3) Avrupa’da UWB için bir yönetmelik düzenleme çalışmasını yürütmüştür. UWB teknoloji 7,5 GHz gibi aşırı bant genişliğini, kısa mesafede düşük güç ile kullanır. IEEE 802.15.3a grubu UWB teknolojinin standardını oluşturmaktadır.

Çizelge 5.4. UWB karakteristikleri (Lee, Su, vd., 2007)

|  |  |
| --- | --- |
| **Standart** | **UWB** |
| IEEE standardı | 802.15.3a |
| Frekans bandı | 3.1-10.6 GHz |
| Maksimum sinyal oranı | 110 Mbps |
| Nominal aralık | 10 m |
| Nominal TX gücü | 41.3 dBm/MHz |
| RF kanal sayısı | (1-15) |
| Modülasyon tipi | BPSK, QPSK |
| Yayılım | DS-UWB, MB-OFDM |
| Şifreleme | AES blok şifreleme |

Uzaysal kanal kapasitesi bakımından (birim kare başına birim saniyedeki bit sayısı,bit/s/m2) IEEE 802.11.ve Bluetooth gibi diğer kısa mesafe kablosuz teknolojilerinden daha üstün performans göstermektedir. Araştırmacılar tarafından sunulan iki çeşit UWB tekniği mevcuttur. Birincisi Doğrudan Dizili Ultra Genişbant (DS-UWB) diğeri ise Çoklu Bantlı Dik Frekans Bölmeli Çoklama (OFDM) tekniğidir. DS-UWB tek taşıyıcılı bir teknik olmasına karşın OFDM çoklu taşıyıcılı bir tekniktir.

* + 1. **WiMAX**

WiMAX (Worldwide Interoperability Microwave Access) dünya genelinde sistemlerin birbiriyle uyumlu halde çalışıp mikrodalga erişim sağlaması amacıyla geliştirilen teknolojidir. WiMAX, 802.16x ve ETSI HiperMAN standartlarına dayanan geniş bandda kablosuz ağlara erişmek için kullanılan teknolojidir. Sabit geniş band teknolojisinin kurulumunun zor olduğu yerlerde, yâda şehirlerde hizmet veren şirketlerin kendi bölgesel şebekeleri arasında hızlı ve güvenilir haberleşme altyapısı oluşturmasını sağlar. Bir başka deyişle WiMAX, Metropol Ağ temeli üzerine kurulmuş teknolojidir. IEEE 802.16 standardı ve uygulanan teknoloji WiMAX ile yüksek veri iletim hızlarında büyük kapsama alanlarında çok sayıda kullanıcıya hizmet verilmesi hedeflenmektedir.

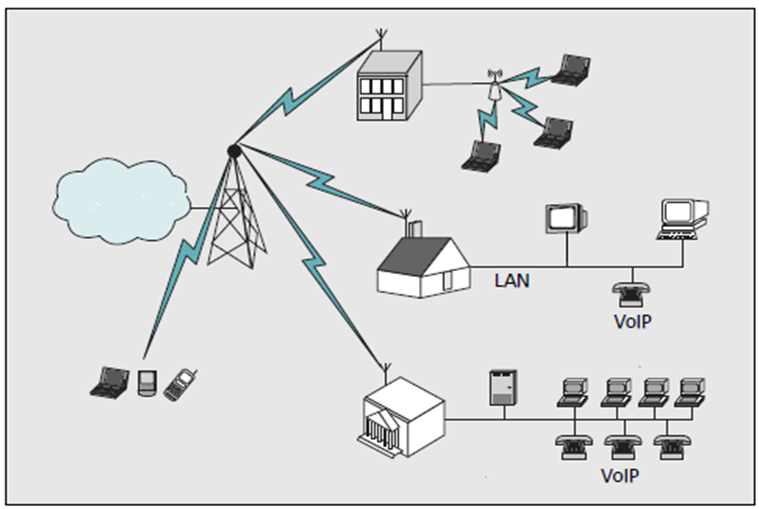
IEEE 802.16 standardı sayesinde ve WIMAX ile yüksek veri iletimi ile kablosuz ağlara geniş bir alanda çok sayıda kişiye hizmet vermek amacı ön plana çıkmaktadır. Buna paralel DSL yada Wi-Fi teknolojilerinin ulaşamadığı yerlerde kablosuz haberleşmenin sağlanması hedeflenmektedir. Amaçlardan biriside, WiMAX ağlarla hücresel ağlarla kablosuz ağların (Wi-Fi) birlikte çalışmasını da sağlamaktır. Çizelge 5.5.’de WiMAX standartlarının özellikleri verilmiştir.

Çizelge 5.5. IEEE 802.16 Standartları (Mohammed, Zaki vd., 2010)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **IEEE**  **802.16 e-2005** | **IEEE 802.16**  **2004** | **IEEE**  **802.16a** | **IEEE 802.16- 2001** |
| **Tamamlanış** | Aralık 2001 | Ocak 2003 | Haziran 2004 | Aralık 2005 |
| **Spektrum** | 10 – 66 GHz | 2 – 11GHz | 2 – 11 GHz | 2-6 GHz |
| **Propagasyon/ Kanal Durumu** | LOS | NLOS | NLOS | NLOS |
| **Modülasyon** | 134  Mbps (28 MHz  Kanallama) | 75 Mbps  (20 MHz  Kanallama ) | 75Mbps  (20 MHz  Kanallama) | 5 Mbps  (5 MHz  Kanallama) |
| **Modülasyon** | QPSK,  16-QAM,  (isteğe bağlı  UL)  ,64-QAM  (isteğe bağlı) | BPSK,  QPSK,  16-QAM,  64-QAM,  256-QAM  (isteğe bağlı) | 256  Alttaşıyıcılı  OFDM,  BPSK,  QPSK,  16-QAM,  64-QAM,  256-QAM | Ölçülendirilebilir  OFMA,  QPSK,  16-QAM  64-QAM,  256-QAM  (isteğe bağlı) |

Çizelge 5.16. WiMAX ve Wi-Fi karşılaştırması (Mohammed, Zaki vd., 2010)

|  |  |  |  |
| --- | --- | --- | --- |
|  | Wi-Fi | WiMAX | |
| Standard | IEEE 802.11 | IEEE802.16 | |
| Kanal genişliği | 20 Mbps’de sabit | Değişken ≤28 Mbps | Değişken ≤20 Mbps |
| Spektrum | 2.4/5.2 GHz | 10-66 GHz | 2-11 GHz |
| Data Oranı | 2/54 Mbps | 240 Mbps | 70 Mbps |
| Genişlik | 100m | 12-15 km | 1-7 km |



Baz İstasyonu

Mobil Kullanıcılar

İç

Network

Ev

Video Akışı

Server ve Bilgisayarlar

İnternet Hotspot

Şekil 5.19. WiMEX kurulumu (Li ve Quin, 2007)

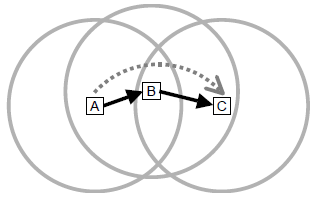
* + 1. **Mesh Network**

Gelecekte kullanılacak servis yapıları, yüksek veri oranlarına cevap vermeye, gönderilen ve alınan verilerde istenilen standartları esnek bir şekilde düşük maliyet ve ekipmanla karşılamaya ihtiyaç duyacaktır. İşte bu noktada Kablosuz Mesh Ağlar (Wireless Mesh Networks - WMNs) teknolojisi ortaya çıkmıştır. Yeni bir teknoloji olup mobil ağlar içinde önemli bir yer edinmiştir.

Bir multihop kablosuz ad hoc ağ içinde, mobil düğümleri Access point veya baz istasyonlarının yardımı olmaksızın bir networkte işbirliği içinde görev yapan önemli ağ türlerindendir. Mobil düğümleri yerine, her biri için sonraki paketler, birbirlerinin direk kablosuz iletişim sırasının ötesinde müsaade edilen sonraki emsal mobil düğümlerin sayısı aracılığıyla mümkün olabilir multihop rotaları üzerinden iletişim kurarlar. Şekil 5.20.’de A B üzerinden C ile iletişim kurmaktadır. (Marsic, 2010)

WMNs’in temel özellikleri:

* Kablosuz ağlardaki problem çözme yöntemlerinin uygulanması ile birden fazla düğümden paketleri göndererek kayıp oranı minimuma indirilebilir,
* Ağa sonradan eklemeler yapılabilmektedir,
* Var olan kablosuz ağ teknolojileriyle uyumludur,
* Düğümler hareketlerinde serbestliğine sahip olduklarından dinamik yapıya sahiptirler,
* Tüm düğümlerin bir yönlendirme protokolüne katılması gerekir.



Şekil 5.20. Örnek kablosuz mesh network (Marsic, 2010)

1. **Mesh Networkler için Yönlendirme Protokolleri**

Kablolu ağ’lar içinde sabit altyapıyla, bir iletişim son nokta aygıtı, bilindiği gibi “host”, yönlendirme protokollerine dahil değildir. Bir kaynak hostundan hedef hostuna ileten paketlerin bir arabirim hesaplayıcı “düğümleri” olarak ayarlanmıştır. Diğer taraftan, kablosuz mesh ağ’lar ortak olarak düğüm hesaplamasında “host” ve “ağ” ‘ın ikisini de almaktadır.

MANET için önerilen çok sayıda yeni yönlendirme protokolü vardır. Bu protokollerin çoğu aslında kablolu iletişim tekniklerine de bağlıdır. Burada yönlendirme protokolleri için iki ana sınıf vardır:

**Proaktif:**

* Network içindeki bilgiye erişilebilir, sürekli güncellemeli
* Yönlendirmeye ihtiyaç duyulduğunda, hemen mevcut
* Perkins ve Bhagwat tarafından DSDV
* Hedef sıralı uzaklık vektörü

**Reaktif:**

* Yalnızca ihtiyaç duyulduğunda aktif duruma geçen yapıdadır
* Yönlendirmeyi sürdürme geçersiz yollar hakkında bilgi sağlamak için gereklidir
* Johnson ve Maltz tarafından DSR
* Perkins veRoyer tarafından AODV

1. **Dynamic Source Routing (DSR) Protokol**

Kaynak yönlendirmesinin anlamı gönderici hedefe yönlendirme sırasında tam sıçrama sırasının bilinmek zorunda olduğudur. DSR ad hoc ağ yönlendirme protokolü bir reaktif (on-demand) protokoldür, dolayısıyla periyodik yönetim güncellemeleri gönderilmesi aracılığıyla, sürekli zeminde işlemleri devam ettirmek yerine ihtiyaç yükseldiğinde yalnızca aktive olmaktadır. DSR yönlendirme problemlerini iki parçada çözmektedir: *RouteDiscovery ve RouteManintance*. Her iki çözüm yönetime de on-demand sistemi ile çalışmaktadır. (Marsic, 2010)

1. **KABLOSUZ SİSTEMLERDE YAYGIN OLARAK KULLANILAN CİHAZLAR**

Kablosuz iletişimi gerçekleştirebilmek için çeşitli firmalar tarafından yetenekli cihazlar tasarlanmaktadır. Bu konuda yaygın olarak kullanılan kablosuz iletişim sistemleri incelenecektir.

**6.1 Erişim Cihazları (Access Point-AP)**

Erişim noktası (AP) kablosuz LAN sistemlerinin kurulumunda önemli bir yeri olan ve kapsama alanı dahilinde tüm trafiği denetlemektedir. AP üzerinde bulunan anten yada antenlerle havadan kablosuz erişimi, kablolu ağa bütünleştirme işlemini de Ethernet gibi LAN teknolojisi ile yapmaktadır.

AP cihazlarında dikkat edilecek özellikler:

* Desteklediği standartlar (802.11a/b/g/n…)
* Desteklediği modülasyon türü (OFDM, 16-QAM, 64-QAM …)
* Veri transfer hızı ( Mbps)
* Ağ bağlantı türü (Infrastructure ve Ad-hoc).
* Çalıştığı frekans aralığı (GHz türünden)
* Cihazın iletim gücü (dBm)
* Alıcı Hassasiyeti (dB)
* Dış anten tipi (adet, Kazanç dBi)
* Desteklediği güvenlik modları (WEP, WPA, WPA2 …)
* Kapalı ve açık alanda çalışma menzili





Şekil 6.1. AP cihazları

* 1. **Kablosuz Ağ Adaptörleri**

Günümüzde, üretilen dizüstü bilgisayarların tamamına yakınında üzerinde kablosuz ağ erişimi bulunmaktadır. Daha eski bir model bilgisayarlarda, Wi-Fi, IEEE 802.11b/g/a/n yâda WLAN adaptör gibi farklı isimlerle satılan PCMCI veya USB adaptörlerle kablosuz ağlara girilebilmektedir.



Şekil 6.2. Kablosuz ağ adaptörleri



PCMCI ağ adaptörü

USB ağ adaptörü

AP’de olduğu gibi Ağ adaptörünün seçiminde de desteklediği standartlar, desteklediği modülasyon türü, veri transfer hızı vb. özelliklere dikkat edilmelidir.

* 1. **Bluetooth Aygıtı**

Çoğu dizüstü bilgisayarda tümleşik olarak bluetooth aygıtı bulunmakla birlikte, haricen de bilgisayara takılabilen bu aygıtlarla bluetooth ağına girilebilmektedir.

Bluetooth aygıtları alınırken:

Açık ve kapalı alanlardaki menzil uzaklığı, frekans aralığı, data transfer hızı vb. özelliklerine dikkat edilmelidir.

Şekil 6.3. Bluetooth aygıtları



* 1. **Ağ Genişletici Adaptör**

Router yada AP’nin ulaşamadığı alanlarda da kablosuz bağlantı sinyalini taşıyarak mevcut kablosuz alanı genişleten aygıtlardır. Bu sistemler uyumlu oldukları kablosuz ağ standartlarına (802.11 b/g/n) bağlı olarak genişletilmiş kapsama alanı içinde kablosuz veri aktarımını gerçekleştirebilmektedir. Üzerlerinde bulunan LAN portları sayesinde kablolu modemleri kablosuz hale getirebilmektedir. MIMO teknolojisine sahip olanlar kablosuz alandaki kör noktaları azaltır ve kablosuz alanı genişletir. Aynı zamanda WEP, WPA, WPA-2 128-bit şifreleme özelliklerine de sahip olabilmektedir.



Şekil 6.4. Ağ genişletici adaptör

1. **SONUÇ**

Bu çalışmada OSI modeli, kablosuz iletişim, kablosuz ağ türleri, kablosuz ağ protokolleri ve kablosuz ağlarda güvenlik gibi konular incelenmiştir. Kablosuz ağ protokolleri anlatılmadan önce OSI modeli, kablosuz iletişimde katmanların fonksiyonları, kablosuz ağ türleri anlatılarak gerekli altyapısı oluşturulmaya çalışılmıştır.

Kablosuz iletişimin teknolojik gelişimi incelenmiş kablosuz ağ standartlarının birlerine göre üstünlükleri ve güvenlik konuları açıklanmıştır. Böylece her geçen gün kullanım oranları artan kablosuz ağ sistemlerinin teknik altyapısı tanıtılmıştır.

# KAYNAKLAR

Afrancheh H.R., Haghighat A. T., 2010, Adaptive Controlling of IEEE 802.16 WiMAX standard and IEEE 802.11 Wireless LAN Networks standard”, IEEE

Borja D., Ferrer-Gomila J., Femenias G., 2008, “Cross-Layer Architecture Design İn Wireless Networks”, Mobile Communication Group

“Cisco 802.11n Technical Overwiev”, 2007

Callaway E., Gorday P., Hester L., 2002, “IEEE Communications Magazine”

Da˜nobeitia-Paul B., Ferrer-Gomila J. L., Femenias G., 2008, ” Cross-layer architecture design in wireless networks”, Mobile Communication Group

Demir S., 2005, “Bilgisayar Ağlari Veri Haberleşmesi Hatalarinin Yapay Sinir Ağlari Teknikleri İle Analizi”, Yüksek Lisans Tezi

Dhawan S., 2007, “Analogy of Promising Wireless Technologies on Different Frequencies: Bluetooth, WiFi, and WiMAX”, The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007)

Gast M.S., “802.11 Protocol Map”

Gast M.S., 2002, “802.11 Wireless Networks”, ISBN: 0-596-00183-5

D.M.GEZGİN, E.BULUŞ, 2009, "RC4 tabanlı WPA(wi-fi protected Access)'da kullanılan TKIP (Temporal Key Integrity Protocol) şifrelemesinin incelenmesi",sf 107-112, IV.İletişim Teknolojileri Ulusal Sempozyumu, Adana-TÜRKİYE

Holt A., Huang C., 2010 “802.11 Wireless Networks”, UK

Howlader M., Kiger C.J., Ewing P.D., 2007 “Coexistence Assessment of Industrial Wireless Protocols in the Nuclear Facility Environment”

Lee J. S., Su Y.W., Shen C.C. , 2007, “A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee, andWi-Fi”, The 33rd Annual Conference of the IEEE Industrial Electronics Society (IECON), Taiwan

Lashakari A.H.,Danesh M.M.S., Samadi B., 2009 “A Survey on Wireless Security protocols (WEP,WPA and WPA2/802.11i)”, IEEE Computer Society

Li B, Qin Y., Low C.P. vd., 2007, “A Survey on Mobile WiMAX”, IEEE Communications Magazine

Li M., Lou W. Ren K., 2010 “DATA SECURITY AND PRIVACY IN WIRELESS BODY AREA NETWORKS”, IEEE Wireless Communications

Lim C., Luo H., Choi C.H. 2006, “RAIN: A Reliable Wireless Network Architecture”, IEEE

Lu K., Qian Y., Chen H. H., 2007, “IEEE Communications Magazine”

Marsic I. , 2010, ”Computer Networks” , Rutgers University, New Jersey

“TCP/IP VE IP Adresleme”, 2008, Megep, Ankara

TCP/IP Overview, Document ID:13769, Cisco System Inc., 2005

Mohamed M.A., Zaki F.W., Mosbeh R.H., 2010, “Simulation of WiMAX Physical Layer: IEEE 802.16e”, IJCSNS International Journal of Computer Science and Network Security, 10, 10

Nabipoor M., 2010, “Controlling and Evaluating of IEEE 802.16 WiMAX standard”, 2010 2nd International Conference on Software Technology and Engineering(ICSTE), IEEE

RS9110-N-11-26 – 802.11abgn Wireless Device Server, Data Sheet, 2011

Pang Q., C.L. Soung, 2005, “Design of an Effective Loss-Distinguishable MAC Protocol for 802.11 WLAN”, IEEE Communications Letter, 9,9

Qu F., Wang F. Y., Yang L., 2010, “Intelligent Transportation Spaces: Vehicles, Traffic, Communications, and Beyond”, IEEE Communications Magazine

Redpine Signals, “RS9110-N-11-26 – 802.11abgn Wireless Device Server” Data Sheet, 2011

Scarfone K, Dicoi D., Sexton M vd., 2008 “Guide to Securing Legacy IEEE 802.11 Wireless Networks”

Scarfone K.,Padgette J, 2008, “Guide to Bluetooth Security”

Sikora A., 2004 “Design challenges for short-range wireless networks”, IEEE Proc.-Common

Sud S.,Want R., Pering T. vd. , 2008, “EnablingRapid Wireless System Composition through Layer-2 Discovery”, IEEE Network

Şekercioğlu Y.A., Ivanovich M., Yeğin A., 2009, “A survey of MAC based QoS implementations for WiMAX networks”, Computer Networks 53, 2517-2536

Tran M., Zaggoulos G., Nix A. vd., 2008, ” Mobile WiMAX: Performance Analysis and Comparison with Experimental Results”, IEEE

WLAN Design Guide, Agilent Technologies, 2005

Wu H., Zhabg Q., 2007, “SoftMAC: Layer 2.5 Collaborative MAC for Multimedia Support in Multihop Wireless Networks”, IEEE Transactions On Mobile Computing, 6,1

www. lerningnetwork.cisco.com, OSI Model Concepts

Yuksel M, 2010 “Meta-Headers: Top-Down Networking Architecture with Application-Specific Constraints”, IEEE Globecom 2010 Workshop on Network of the Future