T.C.
BAHÇEŞEHİR ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

KABLOSUZ AĞLARDA GÜVENLİK

Ercan REİSOĞLU
Bilgisayar Mühendisliği Anabilim Dalı
Bilgi Teknolojileri Programı

Ocak, 2008

İSTANBUL

T.C.
BAHÇEŞEHİR ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

KABLOSUZ AĞLARDA GÜVENLİK

Ercan REİSOĞLU
Bilgisayar Mühendisliği Anabilim Dalı
Bilgi Teknolojileri Programı

Danışman
Yrd. Doç. YALÇIN ÇEKİÇ

Ocak, 2008

İSTANBUL

T.C.
BAHÇEŞEHİR ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİ TEKNOLOJİLERİ

Tezin Adı: Kablosuz Ağlarda Güvenlik
Öğrencinin Adı Soyadı: Ercan Reisoğlu
Tez Savunma Tarihi: 29 Ocak 2008

Bu tezin Yüksek Lisans tezi olarak gerekli şartları yerine getirmiş olduğu Enstitümüz tarafından onaylanmıştır.

Doç. Dr. İrini DİMİTRİYADİS
Enstitü Müdürü
İmza

Bu tezin Yüksek Lisans tezi olarak gerekli şartları yerine getirmiş olduğunu onaylarım.

Yrd. Doç. Dr. Orhan GÖKÇÖL
Program Koordinatörü
İmza

.

Bu Tez tarafımızca okunmuş, nitelik ve içerik açısından bir Yüksek Lisans tezi olarak yeterli görülmüş ve kabul edilmiştir.

Jüri Üyeleri	İmzalar
Yrd. Doç. Dr.Yalçın ÇEKİÇ Tez Danışmanı	----------
Doç. Dr. Ayhan ALBOSTAN Üye	----------
Yrd. Doç. Dr. Levent EREN Üye	----------

ÖNSÖZ

Yüksek lisans öğrenimim sırasında ve tez çalışmalarım boyunca gösterdiği her türlü destek ve paylaştığı görüşlerinden dolayı çok değerli hocam Yrd. Doç. Dr. Yalçın Çekiç'e en içten dileklerimle teşekkür ederim.

Eğitim konusunda beni destekleyen değerli büyüğüm Doç. Dr. M. Emin Karaaslan'a, bu çalışma boyunca yardımlarını esirgemeyen arkadaşlarıma ve çalışmamı destekleyen Bahçeşehir Üniversitesi'ne teşekkürü borç bilirim. Çalışmamın tüm ilgililere yararlı olmasını dilerim.

Ocak, 2008 **Ercan REİSOĞLU**

İÇİNDEKİLER

ŞEKİL LİSTESİ

TABLO LİSTESİ

KISALTMA LİSTESİ

AES (Advanced Encryption Standard) : Gelişmiş şifreleme standardı
AP (Access Point) : Erişim noktası
ARP (Address Resulotion Protocol) : Adres çözümleme protokolü
ASCII (American National Standard Code for Information Interchange): Bilgi değişimi için Amerikan standart kodlama sistemi
BCD (Binary-Coded Decimal) : İkili kod onlusu
BSS (Basic Service Set) : Temel hizmet seti
CBC-MAC (Cipher Block Chaining Message Authentication Code Protocol) : Zincirleme blok şifreleme mesaj doğrulama kodu
CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) : Sayaç modu ile zincirleme blok şifreleme mesaj doğrulama kodu
CDMA (Code Division Multiple Access) : Kod bölüşümlü çoklu erişim
CDPD (Cellular Digital Packet Data) : Hücresel sayısal paket veri
CRC (Cyclic Redundancy Check) : Döngüsel yineleme sınaması
CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) : Taşıyıcı algılaması çoklu erişim/çakışma kaçınma
CSMA/CD (Carrier Sense Multiple Access/Collision Detection) : Çoklu erişimce çarpışmanın tespiti
DCE (Data Communication Equipment) : Veri iletişim donatımı
DoS (Denial of Service) : Bir servisin kullanılmaz hale getirilmesi
DSSS (Direct Sequence Spread Spectrum) : Doğrudan sıralı yayılı spektrumu
DTE (Data Terminal Equipment) : Veri uç birim donatımı
EAP (Extensible Authentication Protocol) : Genişletilebilir doğrulama protokolü
EAP-AKA (Authentication and Key Agreement) : Doğrulama ve anahtar mutabakatı
EAP-MD5 (Message Digest Five) : Mesaj özü
EAPOL (EAP over lan) : EAP kaplamalı yerel ağ
EAP-TLS (Transport Layer Security): Taşıma katmanı güvenliği
EAP-TTLS (Tunneled Transport Layer Security) : Tünellenmiş taşıma katmanı güvenliği
EBCDIC (Extended Binary Coded Decimal Interchange Code): Genişletilmiş ikilik kodlu ondalık değişim kodu
ECC (Error Correction Codes) : Hata düzeltme kodu
FHSS (Frequency-Hopping Spread Spectrum): Frekans atlamalı geniş spektrum
FTP (File Transfer Protocol): Dosya aktarım protokolü
Gbps (Gigabit per second) : Saniyede bir milyar bit
Ghz (Gigahertz): Saniyede bir milyar devir
GSM (Global System for Mobile Communications) : Gezgin iletişim için küresel sistem
GTK (Group Transient Key) : Grup geçiş anahtarı
HTTP (Hypertext Transfer Protocol): Üstmetin aktarım protokolü
IBSS (Independed Basic Service Set) : Bağımsız temel hizmet seti
ICMP (Internet Control Message Protocol) : İnternet kontrol mesajı protokolü
ICV (Integrity Check Value) : Bütünlük kontrol değeri
IEEE (Institute of Electrical and Electronics Engineers) : Elektrik elektronik mühendisleri enstitüsü

IP (Internet Protocol): İnternet Protokolü
ISO (International Standarts Organization) : Uluslararası standartlar organizasyonu
IV (Initialization Vector): Başlangıç vektörü
JPEG (Joint Photographic Experts Group) : Ortak fotoğrafik uzmanlar grubu standardı
KCK (Key Confirmation Key): Anahtar doğrulama anahtarı
KEK (Key Encryption Key) : Anahtar şifreleme anahtarı
LAN (Local Area Networks) : Yerel alan ağları
LEAP (Lightweight Extensible Authentication Protocol) : Sadeleştirilmiş genişletilebilir yetkilendirme protokolü
MAN (Metropolitan Area Network): Kentsel alan ağı
Mbps (Megabit per second) : Saniyede bir milyon bit
MIC (Message Integrity Code) : Mesaj bütünlük kodu
MITM (Man in the Middle): İki iletişim arasına girip veri çalma, değişim yapma gibi işlemlere izin veren saldırı modeli.
MK (Master Key): Ana anahtar
NFS (Network File System) : Ağ dosya yönetim sistemi
NIC (Network Interface Card): Ağ arayüz kartı
OFDM (Orthogonal Frequency Division Multiplexing): Dikey frekans bölüşümlü çoğullama
OSI (Open Systems Interconnection) : Açık sistem bağlantı modeli
PARC (Palo Alto Research Center): Palo Alto araştırma merkezi
PDA (Personal Digital Assistant) : Kişisel dijital yardımcı
PEAP (Protected EAP) : Korunmuş EAP
PMK (Pairwise Master Key): Çiftli ana anahtar
PTK (Pairwise Transient Key) : Çiftli geçiş anahtarı
RADIUS (Remote Authentication Dial-In User Service) : Uzaktan aramalı kullanıcı kimlik doğrulama servisi

RC4 (Rivest Cipher 4) : Ron Rivest simetrik şifreleme algoritması
RF (Radio Frequency) : Radyo frekansı
RSN (Robust Security Network) : Çok güvenli ağ
SMTP (Simple Mail Transfer Protocol) : Basit elektronik posta aktarım protokolü
SPEKE (Simple Password Exponential Key Exchange) : Basit şifre üstel Anahtar değişimi
SSID (Service Set Identifier): Servis seti tanımlayıcı
TCP (Transmission Control Protocol) : İletim kontrol protokolü
TCP/IP (Transmission Control Protocol/Internet Protocol): İletim kontrol protokolü/internet protokolü
TK (Temporal Key): Geçici anahtar
TKIP (Temporal Key Integrity Protocol) : Geçici anahtar bütünlüğü protokolü
TTL (Time to Live): Ömür süresi
UDP (User Datagram Protocol): Kullanıcı datagram protokolü
UTP (Unshielded Twisted Pair) : Kılıfsız büklümlü tel çifti
WAN (Wide Area Network) : Geniş alan ağı
WECA (Wireless Ethernet Compatibility Allience): Kablosuz ethernet uyumluluk birliği
WEP (Wired Equivalent Privacy): Kabloluya eşdeğer gizlilik
Wi-fi (Wireless Fidelity Alliance) : Kablosuz sadakat birliği
WLAN (Wireless Local Area Network): Kablosuz yerel alan ağları
WMAN (Wireless Metropolitan Area Network): Kablosuz anakent alanı ağları

WPA (Wi-fi Protected Access) : Wi-Fi korumalı erişim
WPA2 : Wi-Fi korumalı erişim ikinci sürüm
WPAN (Wireless Personel Area Netwok): Kablosuz kişisel alan ağları
WWAN (Wireless Wide Area Network): Kablosuz geniş alan ağları

ÖZET

KABLOSUZ AĞLARDA GÜVENLİK

Reisoğlu, Ercan

Bilgi Teknolojileri Programı
Tez Danışmanı : Yrd. Doç. Dr. Yalçın Çekiç

Ocak 2008, 76

Kablosuz ağlarda bağlantı hızının kullanıcılar için makul seviyelere çıkması kablosuz ağ kullanımını yaygınlaştırmıştır. Kablosuz ağların geniş bir şekilde kabul görmesi ve bu ağlara olan gereklilik, ağların güvenliği ile ilgili bazi endişeleride beraberinde getirmiştir. Kablosuz ağ güvenliği için birçok yöntem mevcuttur ve her geçen gün geliştirilmektedir. Kullanılan bu yöntemlerden bazıları güvenlik açıklarına sahiptir. Bu açıklardan dolayı kablolu ağlarda tehdit altındadır.

Bu çalışmada yaygın olarak kullanılan bilgisayar ağ yapıları ve ağ standardları anlatılmış, kablosuz yerel ağ standardı ve güvenlik yöntemleri üzerinde durulmuştur. Mevcut kablosuz ağ güvenlik yöntemleri irdelenmiş, kişisel ve kurumsal yöntemler açıklanmıştır. Ağ güvenliğinde seçilecek yöntemler karşılaştırılmıştır. Son bölümde kablosuz ağlara yapılan saldırılarda kullanılan saldırı araçlarından örnekler verilmiştir.

Anahtar Kelimeler: Kablosuz Ağ Tehditleri, Kabloluya Eşdeğer Gizlilik, Wi-fi Korumalı Erişim, Çok Güvenli Ağ, 802.1x

ABSTRACT

SECURITY ON THE WIRELESS NETWORKS

Reisoğlu, Ercan

Information Technologies Program
Supervisor : Asst. Prof. Dr. Yalçın Çekiç

Ocak 2008, 76

The increase of users connection speed at satisfactory levels increased the usage of wireless network. A wide acceptance and the need of the wireless networks led to certain concerns regarding the overall security of the networks. There are various methods for wireless network security and they are new improvements everyday. Some of these methods which are put into use have some security gaps. Hence, due to these gaps the wired networks are also under threat.

In this study, widely used computer network structures and network standards are analyzed and wireless local network standards and security methods are explained. The current methods are analyzed, personal and institutional methods are explained as well. Some of the current methods in network security are compared. In the last part, Some of the attack tools used against wireless networks are given as examples to demonstrate some of the attacks.

Keywords: Wireless Network Threats Wired Equivalent Privacy Wi-fi Protected Access, Robust Security Network, 802.1x

1. GİRİŞ

Bilgisayarlar rutin olarak yapılması gereken işlemleri insanlara göre daha çabuk ve hatasız yaparak kullanıcılara yardımcı olmaktadır. 70'li yıllarda bilgisayar maliyetleri çok yüksek olduğu için sadece araştırma merkezleri ve büyük üniversitelerde bulunabilmekte, kısıtlı sayıdaki insanlar bunları kullanabilmekteydi. Hızla gelişen teknolojinin bir sonucu olarak bilgisayarlar günlük hayatımızın vazgeçilmez bir parçası olmuştur. Hızlı teknolojik gelişmeyle bilgisayarlar öncelikle işyerlerinde kullanılmaya başlandı. Gelişen teknolojiye paralel olarak bilgisayar sayısının artmasıyla beraber bunlarda kullanılan programlarda çeşitlilik göstermeye başlamıştır. Bilgisayar programlarındaki önemli bir sektörde bilgisayar oyunlarıdır. Oyun sektörü doğası gereği çocuklara ve gençlere hitap eder, dolayısıyla bilgisayarlar evlerde de hızlı bir şekilde yer edinmiştir. Bu da bilgisayar kullanıcı sayısının artmasını ve insanların bilgisayar konusunda bilinçlenmesini sağlamıştır.

Bilgisayarların artmasıyla beraber bunlarda üretilen bilgilerin karşılıklı olarak değişilmesi ve paylaştırılması ihtiyacı doğmuştur. Buna yönelik olarak bu ihtiyacı gidermek üzere bilgisayarlar birbirine bağlanmıştır. Bilgisayarlar arası bu bağlantıya bilgisayar ağları adı verilmektedir. Bu bağlantı kablolar yardımıyla yapılmaktadır. Dolayısıyla bağlantı fiziksel bir bağlantıdır. Dünyadaki bilgisayarların birbirlerine bağlanarak oluşturdukları en büyük ağa internet adı verilmektedir. Bilgisayarlar arası yapılan bu iletişimin güvenli olması başlı başına önemli bir konudur. Günümüzde bilgisayar boyutları küçülerek taşınabilir hale gelmiştir. Bu tür bilgisayarların birbirleriyle haberleşebilmeleri için kablolu ağ yerine kablosuz iletişim kullanılmaktadır. Bu iletişim türü kullanıcıların hareket kabiliyetini arttırmaktadır. Kablosuz iletişim radyo frekansları üzerinden yapıldığından bilgisayarlar arası taşınan veriler sadece bu haberleşmeyi yapan bilgisayarlara değil etraftaki bilgisayarlara da ulaşmaktadır. Kötü niyetli insanlar kendilerine ulaşan bu sinyalleri dinleyebilirler ve kötü amaçlarla kullanabilirler. Dolayısıyla kablosuz iletişimde güvenlik önemli bir unsurdur. Bu güvenliği sağlayabilmek için iletişimde kullanılan her katmanda

gözetilmelidir. Örnek olarak işletim sisteminde, ağ kart dizaynı ve protokol gösterilebilir.

Bu tezde bilgisayarlar arası kullanılan kablosuz iletişim güvenliği incelenmiştir. Tez dört bölümden oluşmaktadır. İkinci bölümde bilgisayar ağlarının temel yapısı, fiziksel bağlantı türleri, çalışma prensipleri, standartları ve iletişim protokolü hakkında bilgi verilmiştir. Üçüncü bölümde kablosuz ağ türleri, standartları, çalışma şekilleri, kullandıkları güvenlik protokolleri ayrıntılı olarak anlatılmış, güvenlik açıkları üzerinde durulmuştur. Kablosuz ağ tehditleri sınıflandırılmış, tehditlerin nasıl ve ne şekilde gelebileceği anlatılmıştır. Yapılan saldırılarda sıkça kullanılan yöntem ve araçlar gösterilmiştir. Son bölümde ise kablosuz ağlarda güvenliği sağlamak için, sistemi koruma ve saldırgana karşı alınabilecek önlemlerden bahsedilmiştir.

2. BİLGİSAYAR AĞLARI

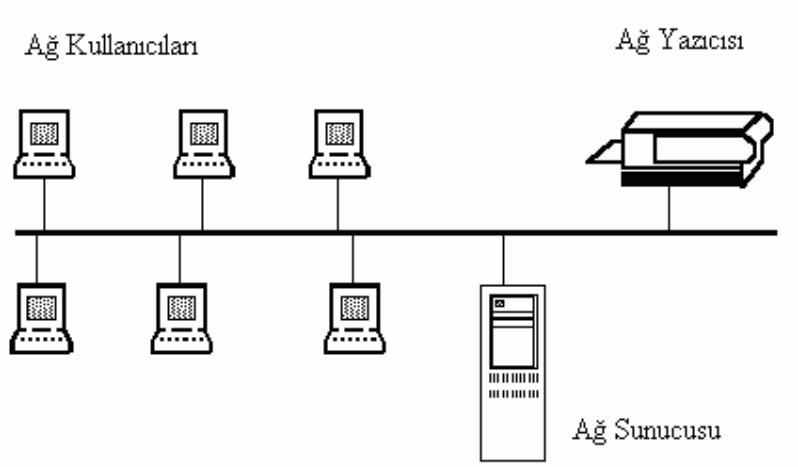
Birden çok bilgisayarın birbirine bağlı olarak kullanılmasıyla oluşturulan çalışma biçimine bilgisayar ağı (computer network) denir. Bir bilgisayar ağında çok sayıda bilgisayar yer alır. Bu bilgisayarlar yan yana duran iki bilgisayar olabileceği gibi tüm dünyaya yayılmış binlerce bilgisayar olabilir. Ağ içindeki bilgisayarlar belli bir biçimde dizilirler. Bilgisayarlar arasında genellikle kablo ile bağlantı sağlanır. Kablo bağlantısının mümkün olmadığı durumlarda mikro dalgalar ve uydular aracılığıyla da ağ içindeki iletişim kurulur. Bilgisayar ağlarının ilk uygulamaları 1960'lı yılların sonlarında başlamıştır. Ancak yerel bilgisayar ağlarının yaygınlaşması 1980'li yıllarda başlamış ve gelişmiştir. 1980'li yıllarda, kişisel bilgisayarların çoğalması, bilgisayar teknolojisindeki ve iletişim teknolojilerindeki gelişmeler bilgisayar ağlarının daha yararlı olmasını sağlamıştır.

Bilgisayar ağı, birbirine bağlı birçok bağımsız bilgisayar anlamına gelir. İki bilgisayarın birbirinin kaynaklarını (diskini ya da diskinde yer alan bilgilerini) paylaşabilmesi ve konuşabilmesi onların birbirine bağlı olduğunu gösterir.

İşletmecilik açısından ağlar, yönetime ve denetime yardımcı olurlar. Bir bankanın ya da üniversitenin çok sayıda bilgisayarı birbirine bağlı olarak kullanılması, onları bağımsız olarak kullanmasından daha anlamlı ve verimli olur. Böylece birimler arası iletişim daha kolay sağlanmakta ve bütünleşik uygulamalar daha kolay gerçekleştirilmektedir. Ortak kaynak kullanımı ile donanım maliyetleri düşer, ortak çalışma imkânını arttırarak takım çalışmalarını hızlandırır, çalışanların verimini ve performansını arttırır. İletişim hızını arttırarak zaman kazancı sağlar, ayrıca önemli bilgilerin yedeklenmesi daha kolay hale gelir.

Bilgisayar ağına bağlı olan bir bilgisayar diğer bilgisayarlarla bağlantı içindedir. Diğer bilgisayarlarla iletişim kurar, onların sabit diskinde yer alan verilere erişir, onların programlarından yararlanır. En basit biçimi ile ağ, genellikle modemlerle birbirine seri bağlantılı olan iki makinedir. Daha karışık ağ yapılarında ise, İletim Kontrol Protokolü /

İnternet Protokolü (TCP/IP-Transmissions Control Protocol / Internet Protocol), protokolü kullanılmaktadır. Bu, yüz binlerce bilgisayarın birbirine bağlı olduğu Internet üzerinde diğer bilgisayarlar ile bağlantı kurmamızı sağlayan protokol ailesidir [1].



Şekil 2.1: Bilgisayar ağ yapısı

Bilgisayar ağları tüm işleme modelleriyle (merkezi, dağıtık ve birlikte) birlikte bilgisayarları ve işletim sistemlerini içerir. Tipik bir ağ, sunucu, istemci, iş istasyonları, yazıcı ve diğer bilgisayar çeşitleri ile ağ cihazlarını içerebilmektedir. Firmaların kullandıkları ağ teknolojileri ve ölçekleri, firmanın yaptığı işle ve firmanın ölçeğiyle paraleldir. Bilgisayar ağları genellikle boyutuna, kapsadığı alana veya yapısına göre sınıflandırılır. Aşağıdaki sınıflandırma ağın kapsadığı alanlara göre yapılmıştır [1, 2].

2.1. YAPILARINA GÖRE BİLGİSAYAR AĞLARI

Bilgisayar ağları, kaynaklara erişim, kapsadığı alan ve söz sahibi olma şekline göre üç gruba ayrılır

2.1.1. Yerel Alan Ağları (LAN-Local Area Network)

Yerel bilgisayar ağları, göreceli olarak küçük olan sistemlerden ve iletişim ortamından oluşur. Yüksek hızlı, küçük alanları (bir bina, bir firma, bir bölüm, bir oda) kapsayan bir veri ağıdır. Yerel ağ içinde bilgisayarlar, sunucular, iş istasyonları, yazıcılar, çiziciler ve diğer çevre birimleri yer alabilir. Normalde tek tür iletişim kuralına eğilim gösterir.

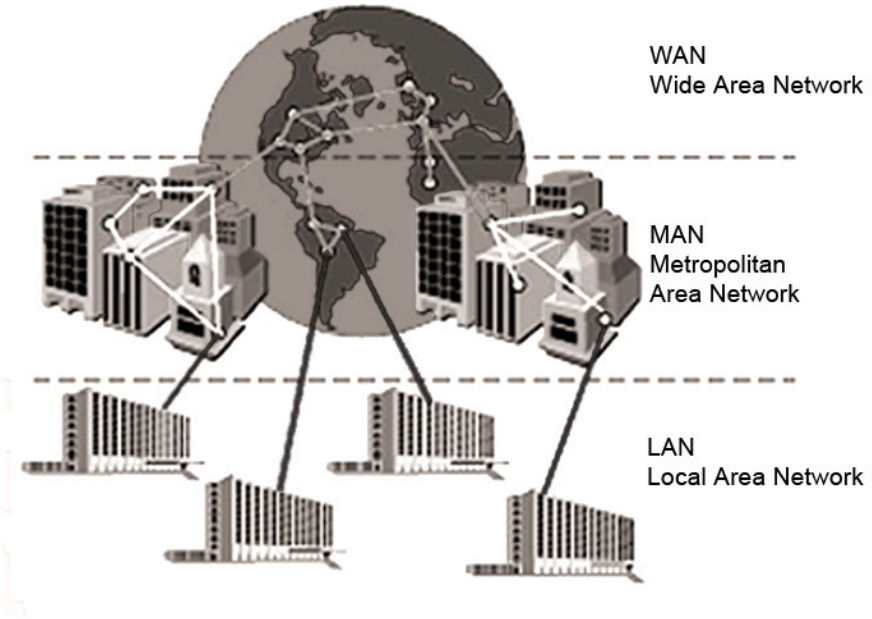
Ancak farklı iletişim kurallarının (ağ protokolleri) kullanıldığı ağlar da mevcuttur. Yerel bilgisayar ağları, genellikle tek bir organizasyon tarafından sahiplenilir ve yönetilirler.

2.1.2. Kentsel Alan Ağı (MAN-Metropolitan Area Network)

Yerel ağlardan daha geniş, genellikle birkaç mevcut yerel bilgisayar ağının birleştirilmesi sonucu kurulan ağlardır. Genelde şehir içi uzak bağlantılar söz konusu olduğundan ve şehrin bir kısmını kapsadığından kentsel ağlar denmiştir. Mesafenin etkin olarak kapsanması gerektiği ve ağa bağlı her bölge arasında tam erişim gerekmediğinden değişik donanım ve aktarım ortamları kullanılır.

2.1.3. Geniş Alan Ağı (WAN-Wide Area Network)

Yerel veya kentsel ağların birleşmesi ile oluşturulurlar. Şehir, ülke, kıta, hatta dünya çapındaki bilgisayarların birbirleriyle ilişkilendirilmesi sonucunda oluşmuş veya kurulmuş olan bilgisayar ağlarıdır. Geniş alan ağı, coğrafi olarak uzak mesafelerdeki kentsel ağdan geniş her tür ağı birbirine bağlamak için kullanılır. Ülkenin ya da dünyanın çeşitli bölgelerindeki yerel alan ağları birbirine bağlayan yapıdır [1, 2, 3].

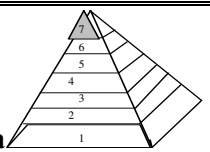
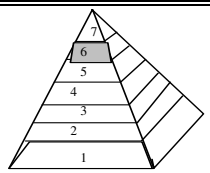
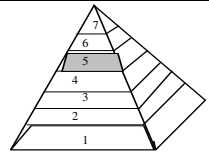
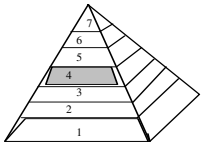
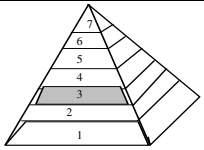
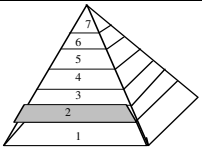
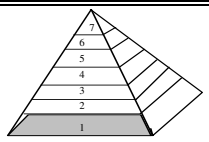


Şekil 2.2: Bilgisayar ağları

2.2. AÇIK SİSTEM BAĞLANTI MODELİ (OSI-OPEN SYSTEMS INTERCONNECTION)

Bilgisayarlar arası iletişimin başladığı günden itibaren farklı bilgisayar sistemlerinin birbirleri arasındaki iletişim daima en büyük problemlerden birisi olmuş ve bu sorunun üstesinden gelebilmek için uzun yıllar boyunca çeşitli çalışmalar yapılmıştır. 1980'li yılların başında Uluslararası Standartlar Organizasyonu (ISO-International Standarts Organization) bilgisayar sistemlerinin birbirleri ile olan iletişiminde ortak bir yapıya ulaşmak yönünde çabaları sonuca bağlamak için bir çalışma başlatmıştır. Bu çalışmalar sonucunda 1984 yılında Açık Sistem Bağlantıları (OSI-Open Systems Interconnection) referans modeli ortaya çıkarılmıştır. Bu model sayesinde değişik bilgisayar firmalarının ürettikleri bilgisayarlar arasındaki iletişimi bir standarda oturtmak ve farklı standartlar arası uyumsuzluk sebebi ile ortaya çıkan iletişim sorununu ortadan kaldırmak hedeflenmiştir. OSI referans modelinde, iki bilgisayar sistemi arasında yapılacak olan iletişim problemini çözmek için 7 katmanlı bir ağ sistemi önerilmiştir. Bir başka deyişle bu temel problem 7 adet küçük probleme bölünmüş ve her bir problem için ayrı bir çözüm yaratılmaya çalışılmıştır. OSI modeli, bir bilgisayarda çalışan uygulama programının, iletişim ortamı üzerinden başka bir bilgisayarda çalışan diğer bir uygulama programı ile olan iletişiminin tüm adımlarını tanımlar. En üst katmanda görüntü ya da yazı seklinde yola çıkan bilgi, alt katmanlara indikçe makine diline dönüşür ve sonuç olarak 1 ve 0'lardan ibaret elektrik sinyalleri halini alır [4].

OSI başvuru modelinin katmanları, uygun katmanlara arayüz oluşturmakta tasarlanmıştı. Örneğin sunum katmanı, Uygulama ve Oturum katmanları arasında arayüz oluşturmak için tasarlanmıştı. Her katman, diğer katmanlardan bağımsız belirgin işlevleri tanımlamaktadır. Bu da iletişim sisteminin bölünmesine izin verir. Böylece ağ mimarisi tasarım işlerliği her katmanda değişik problemlerin tutulmasına izin verir. Burada, tüm işletim sisteminin karmaşıklığı bölünüp basit süreçlere adreslenir. Katmanlı ağ mimarisi bu tarzda işlerliğin çoklu fiziksel aygıtlar arasında ağ tasarımının doğal bölünmesini sağlar. OSI'nin gelişi her türden bilgisayarın birbiri ile iletişimi sorununa çözüm olmuştur. OSI modelinin yedi katmanı vardır [5].

 **Uygulama**	Kullanıcıya en yakın katmandır. Kullanıcının elinin altındaki uygulamaları burada yer alır.
 **Sunum**	Bu katmanda gelen bilginin karakter takımı dönüşümleri, şifreleme gibi işlemleri ile uğraşılır.
 **Oturum**	İki bilgisayar üzerindeki uygulamaların birbirini fark ettiği katmandır.
 **Taşıma**	Burada, gelen bilginin doğruluğu araştırılıp, hatalıysa düzeltilmesine çalışılır.
 **Ağ**	Bağlantıyı sağlayan yönlendirme protokolleri bu katmanda çalışır.
 **Veri Bağı**	Fiziksel adresleme, ağ yerleşim biçimi, akış denetimi gibi işler bu katmanın görevidir.
 **Fiziksel**	Bu katman, modülasyon teknikleri, çalışma voltajı ve sıklık (frenkansı) gibi elektriksel ve mekanik özellikleri belirleyen katmandır.

Şekil 2.3: OSI katmanları

Uygulama Katmanı (Application Layer)

Kullanıcıya en yakın katmandır. Kullanıcı uygulamalarına dosya aktarım, elektronik mektuplaşma, uzaktan dosya erişimi, ağ yönetimi, terminal protokolleri gibi standartlar geliştirilmiştir. Ayrıca uygulamaların birbirleriyle iletişimini kontrol eder. Diğer bilgisayarlar ile haberleşen bir uygulama, OSI uygulama katmanı kavramlarını kullanıyor demektir. Uygulama katmanındaki uygulamaların haberleşme yetenekleri bulunmalıdır. Örneğin, haberleşme yetenekleri bulunmayan bir kelime işlemci programı, haberleşme ile ilgili kodlar içermeyecek ve OSI uygulama katmanı

kullanmayacaktır. Ancak, kelime işlemci programına, dosyaların gönderilmesi gibi bir seçenek eklenirse, kelime işlemci programı OSI uygulama katmanı kullanmak zorunda kalacaktı [5, 6, 7].

OSI uygulama katmanının kullandığı bazı uygulamalar şunlardır;
Telnet, Üstmetin Aktarım Protokolü (HTTP–Hypertext Transfer Protocol), Dosya Aktarım Protokolü (FTP–File Transfer Protocol), Ağ Dosya Yönetim Sistemi (NFS – Network File System), Basit Elektronik Posta Aktarım Protokolü (SMTP – Simple Mail Transfer Protocol).

Sunum Katmanı (Presentation Layer)

Veriyi alıcı cihaz tarafından okunabilir hale getirmekten sorumlu olan katmandır. Gönderilen verinin alıcı cihaz tarafından nasıl okunacağını belirtir. Verinin biçimlendirilmesi, şifrelenmesi ve sıkıştırılması görevini üstlenir [7]. Bu katmanın temel amacı, Bilgi Değişimi İçin Amerikan Standart Kodlama Sistemi (ASCII-American National Standard Code for Information Interchange) metni, Genişletilmiş İkilik kodlu Ondalık Değişim Kodu (EBCDIC-Extended Binary Coded Decimal Interchange Code) metni, İkili Kod Onlusu (BCD-Binary-Coded Decimal) gibi veri formatlarını tanımlamaktır. Şifrelemede, örneğin, FTP kullanırken ikilik ya da ASCII modda iletim yapılması sağlanabilir. Eğer ikilik mod seçilmiş ise, gönderici ve alıcı, dosyanın içeriğini değiştirmez. Eğer ASCII mod seçilmiş ise, gönderilen metni standart ASCII kodlarına dönüştürür ve veriyi gönderir. Alıcı, standart ASCII kodlarını bilgisayarda kullanılan karakter kümesine bağlı olarak yeniden biçimlendirir [6].

Oturum Katmanı (Session Layer)

Uygulamalar arasındaki oturumları başlatır, sonlandırır ve yönetir. Oturum katmanı eşzamanlı olarak iletişimi sağlar. Oturum katmanı, oturum olarak adlandırılan konuşmaların nasıl başlayacağını, biteceğini ve kontrol edileceğini tanımlar. Bu, birden çok iki yönlü mesajın idare ve kontrol edilmesini de kapsar. Bu sayede uygulama, sadece belli mesaj dizisinin iletilmesi tamamlandığında gerekli işlemleri yapmaya başlar. Oturum katmanının, gelen verinin kesintisiz bir görüntüsünü elde edebilmesini de bu sağlar. Örneğin, otomatik para çekme makinelerinde siz parayı almadan, para

hesabınızdan düşürülmez. Oturum katmanı, hangi işlemlerin aynı otururumun parçası olduğunu ve oturumun kapatılabilmesi için hangi işlemlerin tamamlanması gerektiğini belirleyebilir [6].

Taşıma Katmanı (Transport Layer)

Birincil görevi gönderici ve alıcı arasındaki veri akışının kontrolü ve verinin alıcıya ulaştığından emin olmaktır. Alıcı cihazın veriyi almaya hazır olup olmadığı ve veri gönderildikten sonra alıp almadığı gibi kontrollerin yapıldığı katmandır. Burada, gelen bilginin doğruluğu araştırılıp, hatalıysa düzeltilmesine çalışılır. Bu katman güvenilir bir dağıtımdan sorumludur. Bu da dağıtım sunumudur. Daha çok paket dağıtım sunumunu garantilemeye çalışan taşıma katmanı veri dağıtmayı garantiler. Eğer veri "paketi" olarak anılan paket dağıtılmayabilir ise istekte bulunan sunucuya gecikmenin olacağını bildiren bir ileti gönderilir. Dağıtımı garantilemek için kullanılan yöntemler arasında, bilgilendirme iletileri, akış denetimi ve veri paketlerine atanan paket sıra numaraları yer alır. Bu katman iletinin doğru olarak dağıtıldığını garanti etmez. Sadece dağıtıldığını garanti eder. Düzeltmeye gereksinimi olan bir ileti varsa onu yeniden belirlemek ve yeniden göndermek sunum ve oturum katmanının sorumluluğudur [5]. Hata giderme imkânı sunan ya da sunmayan protokollerin seçimine imkân sağlar. Gelen veriyi, aynı makine üzerindeki farklı uygulamalara (örneğin TCP soketlerine) göndermek için çoğullama da bu katmanda yapılır. Sırayı bozan bir paket alındığında, paketin yeniden istenmesi de yine bu katmanda gerçekleştirilir [6].

Ağ Katmanı (Network Layer)

Bu katman, paketlerin uçtan uca gönderimini tanımlar. Ağ katmanı bilgiyi ağa yerleştirmekten sorumludur. Ağ katmanı bunu yapabilmek için, uç noktaların belirlenmesinde kullanılmak üzere mantıksal adresleme yapar. Bu katman sunucu adres alanından kaynaklanan iletileri düzeltir ve daha ileri geçirir. Eğer sınanan sunucu uzak bir sunucu değilse paket, uzak sunucunun yolunu içeren farklı bir ağ dilimine geçirilir (forward). İleti ileri geçirme işlemi yönlendirme ile ilintilidir. Yönlendirme işlemi, iletinin uzaklara erişmesi için en kısa ve en iyi yolun bulunmasıdır. Bilginin aktarılacağı yolun bulunması bir hesaplamaya dayanmaktadır. Sınanan ileti bir sunucu için ise daha ilerde işlenmek üzere taşınma katmanında tutulur. Farklı ortamlarda, iletilebilecek

maksimum veri miktarının farklı olmasından dolayı yaşanan sıkıntıları gidermek amacıyla, bir paketi daha küçük paketlere bölme işlemi de bu katmanda tanımlanır [5, 6].

Veri Bağı Katmanı (Data Link Layer)

Gönderilecek verinin elektronik sinyallere dönüştürülüp kabloya iletilmesine ve kablodan gelen elektronik sinyallerin veriye dönüştürülmesini sağlayan katmandır. Bu dönüştürme işlemi kullanılan ağ teknolojisine göre değişkenlik gösterebilir. Elektronik sinyallerin kablo üzerinde sorunsuz bir şekilde ilerleyip ilerleyemediğinin kontrolü bu katmanda yapılır. Ayrıca bu katmanda fiziksel adresleme yapılır [7]. Fiziksel katmandan gelen bir dizi 0'lar ve 1'ler çerçeve ve paketlere dönüştürülür. Çerçeveler ve paketler, iletilerin kaynak ve varış adresleri, gerçek ileti daha sonraki katmanlarda istenen herhangi bir denetim bilgisini içerir. Veri Bağı katmanı veriyi fiziksel katmana göndermeden önce özel denetim bilgilerini ekler ve bu bilgileri veriyi ağ katmanına göndermeden önce bilgiden soyar alır. Veri bağı katmanında bazı hata düzeltme işleri yapılır. Döngüsel Yineleme Sınaması (CRC-Cyclic Redundancy Check) Hata Düzeltme Kodu (ECC-Error Correction Codes) ile bit hatası yakalanır, düzeltilir [5].

Fiziksel Katman (Physical Layer)

Veri bağı katmanı tarafından elektronik sinyallere dönüştürülen verinin taşınmasından sorumludur. Basit olarak ağ kablosudur. Gerçek kablolama ile bilginin konulması ve alınmasının yapıldığı katmandır. Mekaniksel, kablolama ve elektriksel sinyallerin ayrıntıları burada tutulur. Bunlar kullanılan konnektör bağlayıcı tipi, kullanılan ortamın tipi (eşeksenli, bükülmüş tel çifti veya fiber optik gibi) ve bant genişliğidir. Bu katman duvarlar boyunca koşan kablolar, her bilgisayarın arkasında yer alan bağlayıcılar ve elektriksel sinyallerin özellikleri ile ilgilidir [5].

2.3. ETHERNET KAVRAMI VE STANDARTLARI

Ethernet Xerox'un Palo Alto Research Center (PARC)'da, 1976'da geliştirilmiştir. Ethernet, 1980'de ilk olarak yayınlanan Elektrik Elektronik Mühendisleri Enstitüsü (IEEE-Institute of Electrical and Electronics Engineers) 802.3 standardına teknolojik olarak temel sağlamıştır. Bundan kısa bir süre sonra, Digital Equipment Corporation,

Intel Corporation, ve Xerox Corporation beraberce IEEE 802.3 ile uyumlu bir Ethernet (sürüm 2.0) standardını geliştirdiler ve duyurdular. Ethernet ve IEEE 802.3, birlikte, şu anda yerel ağ protokolleri pazarında en büyük pazar payına sahiptir. Bugün Ethernet terimi genel olarak IEEE 802.3'ün de dahil olduğu Ethernet standartlarına uyan tüm Taşıyıcı Sinyalin Algılanması, Çoklu Erişimce Çarpışmanın Tespiti (CSMA/CD-Carrier Sense Multiple Access/Collision Detection) ağları için kullanılır [8].

İlk geliştirildiğinde Ethernet, uzun mesafeli düşük hızlı ağlar ve özel, yüksek hızlı veri taşıyan ancak mesafe kısıtlaması olan bilgisayar odası ağları arasındaki boşluğu doldurmak için tasarlanmıştı. Ethernet, yerel haberleşme ortamının dağınık bazen yüksek oranda ağır trafik taşıması gereken uygulamalar için uygundur [8].

Ethernet veriyi elektrik sinyaliyle kodlar. 10 Mbps (Megabit per second-Saniyede Saniyede Bir Milyon Bit) sistemlerde kodlama biçimine Manchester kodlaması denir. Bu sistem voltajda değişiklik yaparak ikilik sayıları sıfır ve bir olarak gösterir. Bir zaman diliminde voltajdaki artış ya da düşüşe bit periyodu denir, bitin ikili sayı değerini gösterir [9].

Ethernet'ler, kullanılan kablo ve iletişim hızlarına göre ayrıca sınıflandırılırlar. 10 Mbps hızıyla haberleşenler genel olarak Ethernet, 100 Mbps hızıyla haberleşenler Fast Ethernet, 1000 Mbps hızıyla haberleşenler Gigabit Ethernet olarak isimlendirilirler [10, 11].

Ethernet Ağ Elemanları

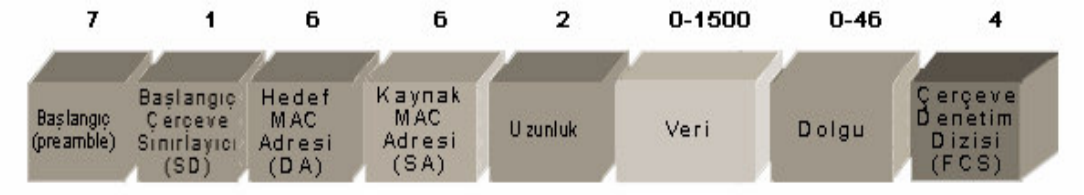
Ethernet yerel ağları, ağ boğumlarını (nodes) ve fiziksel bağlantı medyalarını içerir. Veri Uç Birim Donatımı (DTE - Data Terminal Equipment) ve Veri İletişim Donatımı (DCE - Data Communication Equipment) olarak başlıca iki gruba ayrılırlar. Aygıtlar veri çerçevelerinin hedefi ya da kaynağı olabilir. DTE aygıtları kişisel bilgisayarlar, iş istasyonları ve dosya sunucuları olabilir. DCE aygıtları gelen veri çerçevelerini ağa ileten cihazlardır. Ağ anahtarları (network switch), yineleyici (repeater) ve modemler DCE aygıtlarıdır [10].

Taşıyıcı Sinyalin Algılanması, Çoklu Erişimce Çarpışmanın Tespiti (CSMA/CD - Carrier Sense Multiple Access/Collision Detection)

Ethernet'te veri iletim yoluna erişmek (fiziksel ortama giriş) için kullanılan tekniktir. Ethernet, bir tümegönderim (broadcast network) teknolojisidir. Bu teknik veri iletim yoluna bağlı tüm birimlerin ağ ortamına erişmesini sağlar. Sadece bir düğüm belli bir zamanda ağı kullanmaya elverişlidir. Bu kavramda bir istasyon ağa bir çerçeve iletmek istediğinde ağın başka bir istasyon tarafından kullanılmadığından emin olmalıdır. Veri iletim yolu, bağlı olan tüm birimlerin veri aktarımına açık olduğu için aynı anda farklı birimler tarafından veri aktarılmaya çalışılması çatışmaya (collision) neden olur. Çatışma durumunda tüm veriler bozulur ve yeniden aktarılması gerekir. Bu nedenle veri gönderen bir düğümün aktarım sonrası hattı dinlemesi ve olası çatışmaların farkına varması gerekir. Çarpışma denetimi, veri aktarmak isteyen her iki istasyonun benzerliğini fark eder ve eş zamanlı olarak ağın boş olduğunu tespit edebilir. Her iki istasyonda ağa çerçeve gönderdiğinde milisaniyeler sonra her iki çerçeve çarpışır. Çarpışmalar Ethernet'te normal olaylardır. Böyle bir çarpışma olduğunda iki istasyonda taşımayı durdurur rastgele bir gecikmeden sonra çerçeveyi yeniden gönderir. Gecikmenin rastgele olması önemlidir, aksi takdirde aynı çarpışma çok kez ortaya çıkacaktır. Her iki bilgisayar da çatışmayı sezince, veri aktarımına bir süre ara verip ikili üssel geri çekilme (binary exponential backoff) algoritmasını kullanılarak tekrarlarlar. Ethernet'te kullanılan CSMA/CD, veri çerçevelerini alır ve taşır, veri çerçevelerini OSI üst katmanına geçirmeden önce çözer, adreslerin geçerliğine bakar ve ağda ya da veri çerçevesinde oluşan hataları tesit eder [9, 12, 13].

MAC (Media Access Control - Ortam Erişim Kontrol) Adres Kavramı

Ethernet ağ cihazlarına, 48 bitlik, onaltılık sayı düzeninde ve bir eşi daha olmayan seri numarası verilir. LAN içerisindeki yerel erişimler bu adresler kullanılarak gerçekleşir [14]. Bu numaralar, üretici firmalar tarafından fabrikada verilmektedir. Örnek olarak 12:34:56:78:90:AB bir MAC adresidir. Her üretici firmanın kendi ürünleri için kullanabileceği belli bir MAC adresi alanı vardır [15]. Ethernet çerçeve yapısı Şekil 1.4'de gösterilmiştir [16].



Şekil 2.4: Ethernet çerçeve yapısı

2.3.1. Ethernet Standartları

Tablo 1.1'de Ethernet standartları, kablo tür ve mesafeleri verilmiştir [6].

Tablo 2.1: Ethernet standartları

Standart	Bant Genişliği	Azami Mesafe	Kullanılan Kablo
10Base-2	10 Mbps	185 metre	50 ohm sonlandırıcı ile sonlandırılmış ince koaksiyel (eşeksenel) kablo.
10Base-5	10 Mbps	500 metre	50 ohm sonlandırıcı ile sonlandırılmış kalın koaksiyel kablo.
10Base-T	10 Mbps	100 metre	Kategori 3, Kategori 4, Kategori 5 UTP (Kılıfsız Büklümlü Tel Çifti) kablo.
10Base-F	10 Mbps	2 Km (Kilometre)	Fiber Optik (Optik Lif Kablo)
100Base-TX	100 Mbps	100 metre	Kategori 5 UTP
100Base-T2	100 Mbps	100 metre	Kategori 3, Kategori 4, Kategori 5 UTP
100Base-FX	100 Mbps	400 metre-2000 metre	Fiber Optik
1000Base-LX	1000 Mbps	440 metre-3 Km	Tek Mod veya Çoklu Mod Fiber Optik kablo.
1000Base-SX	1000 Mbps	220 –550 metre	Çoklu Mod Fiber Optik kablo.
1000Base-CX	1000 Mbps	25 metre	Bakır kablo.
1000Base-T	1000 Mbps	100 metre	Kategori 5 UTP

2.3.2. Ağ Topolojileri

Topoloji (bağlantı ve yerleşim biçimi), bilgisayarların birbirine bağlanma şekillerini tanımlayan genel bir terimdir. Yaygın olarak kullanılan topoloji türleri şunlardır;

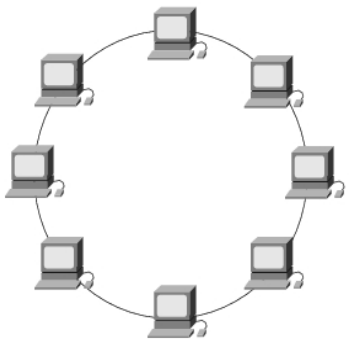
Veriyolu Topoloji (Bus)

Tüm bilgisayarların aynı kabloya bağlı oldukları sistemdir. Tüm bilgisayarlar ortamı dinleyerek kendilerine gelen veriden haberdar olurlar.

Şekil 2.5: Veriyolu topoloji

Halka Topoloji (Ring)

Ağ bir düğümden diğerine geçerek uzar. Düğümler arasındaki bağlantıların mutlaka bir halka oluşturması gerekir. Elektrik sinyali tek yönlüdür. Her noktada sinyal kuvvetlendirilir.



Şekil 2.6: Halka topoloji

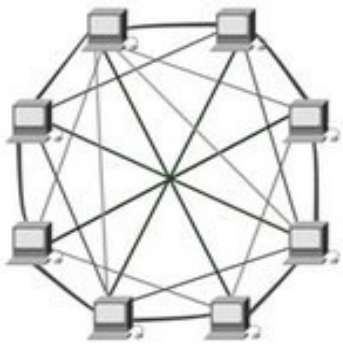
Yıldız Topoloji (Star)

Yıldız ağlarda tüm düğümler merkezdeki bir düğüme bağlanırlar ve düğümler arasındaki haberleşme merkez düğüm üzerinden gerçeklenir.

Şekil 2.7: Yıldız topoloji

Örgü Topoloji (Mesh)

Düğümler arasında bağlantılar oluşturarak, tüm düğümlerden diğerlerine bir kaç yol üzerinden erişimi sağlayan topolojilere örgü (mesh) topoloji oluşturur [12].

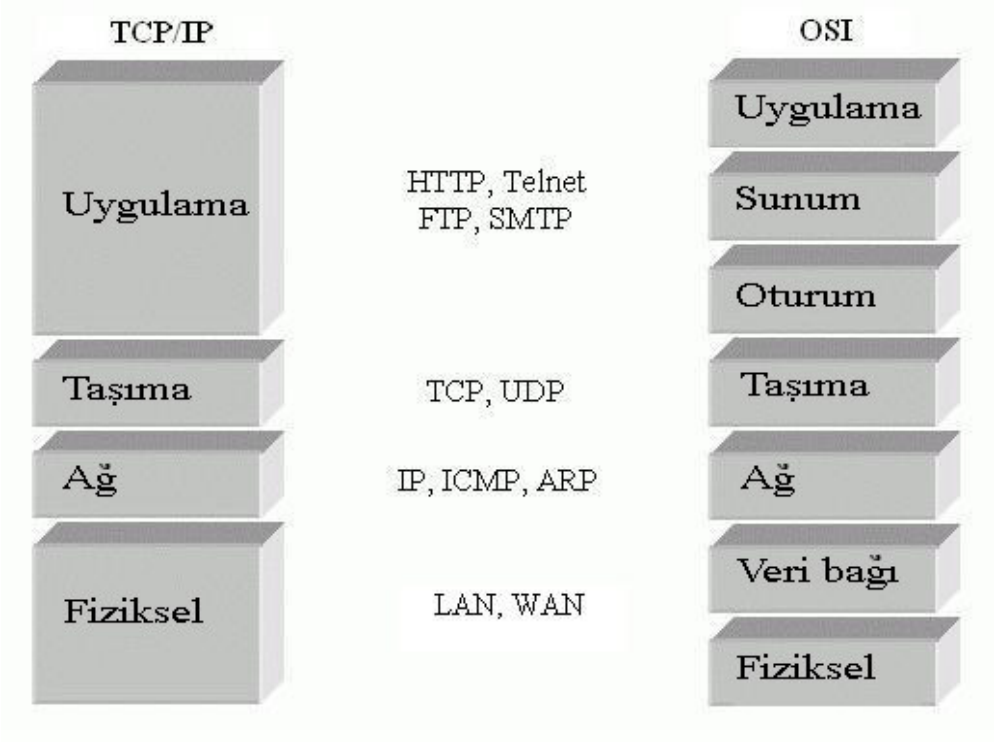


Şekil 2.8: Örgü topoloji

2.4. İLETİM KONTROL PROTOKOLÜ/İNTERNET PROTOKOLÜ (TCP/IP-TRANSMISSION CONTROL PROTOCOL/INTERNET PROTOCOL)

TCP/IP birçok küçük protokolden oluşur. Adını en çok bilinen ikisinden (TCP ve IP) alır [6]. TCP/IP protokol kümesinde yaklaşık 100 protokol bulunur. Birçoğu, IP paketlerinin alt katman protokollerine nasıl taşınacağını gösterir. Setteki anahtar protokoller İletim Kontrol Protokolü (TCP), İnternet Protokolü (IP) ve Kullanıcı Datagram Protokolü'dür (UDP- User Datagram Protocol). TCP/IP ilk günden beri yerel alan ağları, yerel ve geniş alan ağları bağlantısı, bilgisayar ağı yönetimi ve bilgi servisi sağlanması gibi yeni ortaya çıkan konulara hitap etmektedir. Protokol kümesi akla gelebilecek her tip bilgisayara destek vermektedir. TCP/IP'nin kaynak kodu genel ortamda bulunup, kullanımı teşvik edilmektedir [4].

TCP katmanı komutların karşı tarafa ulaştırılmasından sorumludur. Karşı tarafa ne yollandığı ve hatalı yollanan verilerin tekrar yollanmasının kayıtlarını tutarak gerekli kontrolleri yapar. Eğer gönderilecek veri bir kerede gönderilemeyecek kadar büyük ise TCP onu uygun boydaki bölütlere (segment) böler ve bu bölütlerin karşı tarafa doğru sırada, hatasız olarak ulaşmalarını sağlar. TCP ayrı bir katman olarak çalışmakta ve tüm diğer servisler onun üzerinde yer almaktadır. Böylece yeni bir takım uygulamalar da daha kolay geliştirilebilmektedir. Üst seviye uygulama protokollerinin TCP katmanını çağırmaları gibi benzer şekilde TCP'de IP katmanını çağırmaktadır. Ayrıca bazı servisler TCP katmanına ihtiyaç duymamakta ve bunlar direk olarak IP katmanı ile görüşmektedirler. Belirli görevler için belirli hazır yordamlar oluşturulması ve protokol seviyeleri inşa edilmesi stratejisine katmanlaşma adı verilir. En genel haliyle TCP/IP uygulamaları 4 ayrı katman kullanır [17]. Uygulama katmanı altında sırasıyla taşıma, yönlendirme ve fiziksel katman yer alır. Taşıma katmanında TCP ve UDP protokolleri, yönlendirme katmanında IP, İnternet Kontrol Mesajı Protokolü (ICMP-Internet Control Message Protocol), Adres Çözümleme Protokolü (ARP-Address Resolution Protocol) tanımlıdır. Fiziksel katman için varolan tanımlar (Ethernet) geçerlidir [14]. Şekil 9'da TCP/IP mimarisi açıklanmış ve OSI katmanları karşılaştırması gösterilmiştir.



Şekil 2.9: TCP/IP ve OSI karşılaştırması

2.4.1. Uygulama Katmanı Protokolleri

Uygulama katmanı, SMTP, HTTP, FTP, Telnet gibi protokoller üstünde bulunan programlara hizmet verirler [14].

SMTP: Temel elektronik posta olanağını sağlar. SMTP birbirinden ayrı bilgisayarlar arasında bir mesaj aktarımı mekanizmasını üretir. SMTP postalama listesi, kabulleri geri döndürme ve ileriye geçirmeyi (forwarding) içine alan özellikleri taşır. SMTP protokolü mesajların yaratılma yöntemini belirlemez. Mesaj yaratıldıktan sonra, SMTP mesajı alır ve TCP yi kullanarak diğer bilgisayardaki SMTP modülüne gönderir. Hedef SMTP modülü yerel elektronik posta paketini kullanıcının posta kutusuna gelen mesaj olarak koyar [5].

HTTP: Örgü(web) sayfalarının alış verişini sağlar [14].

FTP: Kullanıcıların komutlarına bağlı olarak dosyaları bir sistemden diğerine göndermede kullanılır. Hem ikili hem de metin dosyalarına yer verilir. Protokol

kullanıcı erişimini denetlemek için olanaklar üretir. Kullanıcı dosya aktarımını istediği zaman, FTP denetim mesajlarının değişimi için hedef sisteme TCP bağlantısını hazırlar. Bu durum kullanıcının ID ve anahtar sözcüğünü aktarması kullanıcıya dosyayı belirlemesi ve dosya eyleminin başlatılmasına izin vermek demektir. Bir kez aktarım geliştirildiğinde ikinci bir TCP bağlantısı veri aktarımını hazırlar. Dosya aktarımı veri bağlantısı üzerinden yapılır ve uygulama düzeyinde herhangi bir başlık ve denetim bilgisi yükü getirmez. Aktarım tamamlandığı zaman, bağ denetimi tamamlamayı sinyal eder ve yeni bir dosya aktarım komutu kabul edilir [5].

TELNET: Terminalde ve kişisel bilgisayardaki kullanıcının, uzak bilgisayar ve fonksiyonlarını sanki doğrudan bilgisayara bağlıymış gibi çalışmasına izin verir. Bu protokol basit kaydırma-modu (scroll-mode) terminallerde çalışmak üzere tasarlanmıştır. TELNET gerçekte iki modülde çalışır. Kullanıcı TELNET, terminalin I/O modülü ile etkileşim için yerel terminal ile iletişir. Böylece gerçek terminal karakteristiklerini bilgisayar ağı standartlarına dönüştürür ya da bunun tersi bilgisayar ağı standartları gerçek terminal karekteristiklerine dönüşür. Sunucu TELNET, uygulama ile etkileşir ve uzak terminalin uygulamaya yerelmiş gibi davranmasını sağlar. Kullanıcı TELNET ve sunucu TELNET arasındaki trafik TCP bağlantısı üzerinden sağlanır.

2.4.2. Taşıma Katmanı Protokolleri

TCP/IP'de ulaşım katmanı için TCP ve UDP olarak adlandırılan iki protokol tanımlıdır. TCP bağlantılı düzene dayalı protokoldür. Bağlantılı düzende, gönderici ve alıcı iletişim başlamadan önce birbirleriyle anlaşırlar. İki taraf iletişim yapma konusunda istek ve onaylarını birbirlerine gönderirler. UDP ise bağlantısız düzenli basit bir protokoldür. Bu protokolde iletişim başlamadan önce gönderici ve alıcının bir anlaşmaya varmalarına gerek yoktur [14].

İletim Kontrol Protokolü (TCP-Transmission Control Protocol)

TCP, şu fonksiyonları gerçekleştirmektedir:

- Çoğullama (Multiplexing)
- Hata giderme (Güvenirlik)
- Pencere kaydırma (windowing) kullanarak akış kontrolü

- Bağlantı kurulması ve bağlantının sonlandırılması
- Veri aktarımı

Şekil 2.10: TCP paket formatı

Çoğullama: Gelen verinin hangi uygulamaya verileceğine karar verilme sürecidir [6]. Uygulama katmanı ile taşıma katmanı protokolleri arasında port olarak adlandırılan bir geçit tanımlıdır. Her portun 16 bitlik bir numarası vardır ve her uçta 2^{16} adet port tanımlıdır.16 bitlik port no, bir iletim kontrol protokolü ve 32 bitlik IP adresi soketi oluşturur [14]. Port numaraları 1 ile 65536 arasında yer alır. TCP ve UDP her biri 65,536 portu kullanmıştır [18]. Cihazlar, port numaralarını 1024'ten başlayarak dinamik olarak tahsis ederler. Yaygın olarak bilinen port numaraları (1–1024) sunucular tarafından kullanılır. FTP, Telnet sunucular gibi, bir hizmet sağlayan uygulamalar, yaygın olarak bilinen bir portu kullanarak bir soket açarlar ve bağlantı isteklerini dinlerler. İstemcilerin yaptığı bu bağlantı istekleri hem kaynak hem de hedef port numaralarını içermek zorundadır ve sunucular tarafından kullanılan port numaraları yaygın olarak bilinen portlar olmak zorundadır [6]. 0 ve 255 arası port numaraları,

standart uygulama katmanı hizmetlerine erişim için ayrılmıştır [14]. Port numaraları birden fazla uç-nokta bağlantısı için kullanılabildiğinden, kullanıcılar bir port kaynağını eşzamanlı olarak paylaşabilir [19].

Hata Giderme: TCP güvenli veri aktarımı sağlar. Bu amaçla TCP başlığı içindeki sıra ve onay numaralarını kullanarak veri baytlarını numaralandırır. Her iki doğrultuda da güvenlik sağlar. Bunu bir doğrultuda sıra numarası (squence number) alanını ve diğer doğrultuda onay alanını (acknowledgement field) kullanarak sağlar [6].
Pencere kaydırma (windowing) kullanarak akış kontrolü: TCP akış kontrolünü TCP başlığındaki sıra ve onay numaralarının yanında pencere (window) alanını kullanarak gerçekleştirir [6]. Pencere alanı, TCP penceresinde ne kadar alan olduğunu gösterir. Alış denetimi için kullanılır. 16 bitliktir [19]. Herhangi bir anda izin verilen onaylanmamış en fazla bayt sayısını belirtir. Pencere küçük olarak başlar ve hatalar oluşana kadar büyür. Ağ performansına bağlı olarak yukarı veya aşağıya doğru kayar. Pencere dolu olduğunda, gönderici veri göndermez. Böylelikle veri akışı kontrol edilir. Pencere alanı alıcı tarafından, göndericiye bir sonraki onayı almak için durup beklemeden önce ne kadar veri gönderebileceğini söylemek için kullanılır. Diğer TCP özelliklerinde olduğu gibi, pencere kaydırma simetriktir. Her iki tarafta alır ve gönderir. Pencere kaydırma tüm durumlarda göndericinin iletim yapmayı durdurmasını gerektirmez. Pencere dolmadan önce bir onay alınırsa, yeni bir pencere başlar ve gönderici o pencere dolana kadar veri göndermeye devam eder [6].

Bağlantı kurulması ve bağlantının sonlandırılması: TCP bağlantısı, diğer özellileri çalışmaya başlamadan önce kurulur. Bağlantı kurulması, sıra ve onay alanlarına ilk değerlerin atanması ile kullanılacak port numaraları üzerinde anlaşma sürecidir.

Veri aktarımı: TCP, kaybolan segmentleri yeniden gönderir ve sıralı olarak iletilmemiş segmentleri sırasına koyar. Böylelikle yeniden iletim yapılmasına gerek kalmaz [6].

Kullanıcı Datagram Protokolü (UDP-User Datagram Protocol)

UDP, TCP / IP protokol grubunun iki taşıma katmanı protokolünden birisidir. Gelişmiş bilgisayar ağlarında paket anahtarlamalı bilgisayar iletişiminde bir datagram modu oluşturabilmek için UDP protokolü yazılmıştır. Bu protokol minimum protokol

mekanizmasıyla bir uygulama programından diğerine mesaj göndermek için bir yordam içerir. Bu protokol hareket yönlendirmelidir. Paketin teslim garantisini isteyen uygulamalar TCP protokolünü kullanır. Geniş alan ağlarında (WAN) ses ve görüntü aktarımı gibi gerçek zamanlı veri aktarımlarında UDP kullanılır. UDP bağlantı kurulum işlemlerini, akış kontrolü ve tekrar iletim işlemlerini yapmayarak veri iletim süresini en aza indirir. UDP ve TCP aynı iletişim yolunu kullandıklarında UDP ile yapılan geçek zamanlı veri transferinin servis kalitesi TCP'nin oluşturduğu yüksek veri trafiği nedeniyle azalır. UDP güvenilir olmayan bir aktarım protokolüdür. UDP protokolü ağ üzerinden paketi gönderir ve gidip gitmediğini takip etmez ve paketin yerine ulaşıp ulaşmayacağına onay verme yetkisi yoktur. UDP protokolünü kullanan programlara örnek olarak 161 no' lu portu kullanan SNMP servisini verebiliriz.

UDP datagramların belirli sıralara konmasının gerekli olmadığı uygulamalarda kullanılmak üzere tasarlanmıştır. TCP'de olduğu gibi UDP'de de bir başlık vardır. Ağ yazılımı bu UDP başlığını iletilecek bilginin başına koyar. Ardından UDP bu bilgiyi IP katmanına yollar. IP katmanı kendi başlık bilgisini ve protokol numarasını yerleştirir, bu kez numarası alanına UDP' ye ait değer yazılır. Fakat UDP, TCP'nin yaptıklarının hepsini yapmaz. Bilgi burada datagramlara bölünmez ve yollanan paketlerin kaydı tutulmaz. UDP' nin tek sağladığı port numarasıdır. Böylece pek çok program UDP' yi kullanabilir. Daha az bilgi içerdiğinden UDP başlığı TCP başlığına göre daha kısadır. Başlık, kaynak ve varış port numaraları ile kontrol toplamını içeren tüm bilgidir [20].

Kaynak Port																Hedef Port															
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Uzunluk																Hata Kontrolü															
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Veri																															

Şekil 2.11: UDP paket formatı

UDP ile TCP 'nin Farkları

UDP, gönderilen paketin yerine ulaştığını kontrol etmediğinden güvenilir bir protokol değildir. User Datagram Protocol'ün TCP' den farkı sorgulama ve sınama amaçlı, küçük boyutlu verinin aktarılması için olmasıdır; veri küçük boyutlu olduğu için parçalanmaya

gerek duyulmaz. UDP protokolü ağ üzerinde fazla bant genişliği kaplamaz. UDP başlığı TCP başlığına göre daha kısadır.

Aktarım katmanında UDP'nin oluşturduğu veri bütününe "datagram", TCP'nin oluşturduğu veri bütününe "segment" adı verilir. İkisi arasındaki temel fark, segmenti oluşturan veri grubunun başında sıra numarası bulunmasıdır. Her bir datagram veya segment IP tarafından kendi başlığı eklenerek IP paketi haline getirilir ve herbir IP paketi birbirinden bağımsız olarak hedef cihaza gönderilir. Tablo 1.2'de TCP ile UDP farkları karşılaştırılmıştır.

Tablo 2.2: TCP ile UDP farkları

Servis	TCP	UDP
Bağlantı kurulumu	Zaman alır ancak TCP bunu güvenli şekilde yapar.	Bağlantıya gerek yoktur.
Teslim garantisi	Gönderildiğini onaylar.	UDP onay mesajı göndermeden, alıcı paketin alındığına dair sinyal göndermez. Kaybolan paketler tekrar iletilmez.
Paket ardışıklığı (paketlerin doğru sırası hakkında bilgi)	Ardışık numaralanmış paketler	UDP ardışıklık numarası vermez. Paketlerin sürekli ulaştığı veya kaybolduğu düşünülür.
Akış kontrolü	Alıcı göndericiye yavaşlaması için sinyal gönderebilir.	Paket akış kontrolü için TCP' de kullanılan onay UDP' de geri dönmez.
Tıkanıklık kontrolü	Ağ cihazları TCP onayları sayesinde göndericilerin tavrını kontrol edebilir.	Onay olmadan ağ tıkanıklık sinyali gönderemez.

UDP kullanmanın en önemli nedeni az protokol yüküdür. Video sunucu gibi gerçek zamanlı veri akışı gerektiren bir uygulama için TCP fazla yük getirir ve görüntü gerçek zamanlı oynamaz. Bu nedenle çoğa gönderim(multicast) uygulamalarında datagram

soketler kullanılır. Ayrıca video ve ses görüntülerinde genelde az bir veri kaybı sesi veya görüntüyü bozmaz. Bu nedenle sıkı paket kontrolüne gerek yoktur. Eğer iyi bir fiziksel bağlantınız varsa hata oranı düşük olacaktır ve bu nedenle TCP'nin yaptığı hatalı paket kontrol işlemleri fazladan yük olacaktır [20].

2.4.3. Ağ Katmanı Protokolleri

Yönlendirme katmanında tanımlı protokolleri bir üst katmandan gelen segmentleri alıcıya, uygun yoldan ve hatasız ulaştırmakla yükümlüdür [14].

Adres Çözümleme Protokolü (ARP–Address Resulotion Protocol)

Adres Çözümleme Protokolü (ARP), her tür yayın ağında kullanılabilen OSI birinci katman adresleri ikinci katman adreslere çözümleyen, ikinci katmana ait genel bir protokoldür. Terminaller, yerel alan ağına dahil olduklarında ağ içindeki diğer terminallerle veri alışverişinde bulunabilmek için ARP paketleri yayınlarlar. Bu paketler, ağa dahil olan tüm terminallere ulaşır ancak hedef IP adrese sahip olan terminal bu pakete cevap verir [21]. Yerel ağlarda bir IP paketi gönderebilmek için veri bağı katmanı başlığı ve kuyruğu yaratılmalıdır. Bu yeni başlıktaki kaynak MAC adresi bilinmekte ancak, hedef MAC adresi bilinmemektedir. ARP, IP'nin hedef MAC adresini bulmak için kullandığı metottur [6].

İnternet Kontrol Mesajı Protokolü (ICMP-Internet Control Message Protocol)

ICMP, TCP/IP' nin işlemesine yardımcı olan bilgilendirme protokolüdür. Her düğümde ICMP protokolü çalışır. Hata durumunda düğüm tarafından geri bilgilendirmeyi sağlar. Şu amaçlarla kullanılır;

- Ömür (TTL - Time to Live) süresi dolduğu zaman paketin sahibine bildirim yapmak
- Herhangi bir durumda yok edilen paket hakkında geri bildirim sağlamak
- Parçalanmasın komutu verilmiş paket parçalandığında geri bildirim sağlamak
- Hata oluşumlarında geri bildirim sağlamak
- Paket başka bir yoldan gideceği zaman geri bildirim sağlamak

Güvenilir bir veri dağıtım protokolü değildir. Ortama geri besleme sağlar, IP' yi güvenilir bir protokol haline sokar. IP paketinin veri bölümünde taşınır [22]. ICMP mesaj tipleri Tablo 2.3'de gösterilmiştir [6, 22, 23].

Tablo 2.3: ICMP mesaj tipleri

Mesaj	**Amaç**
Hedefe Erişilemiyor (Destination Unreachable)	Kaynak makineye paketi iletmek ile ilgili bir problem olduğunu bildirir.
Zaman Aşımı (Time Exceed)	Paketi iletmek için harcanan zaman uzamış ve paket düşürülmüştür. Yaşam süresi içerisinde hedefe ulaşmamış paketler son yönlendirici (router) üzerinde yok edilir. Time exceed paketi ile paket sahibi bilgilendirilir.
Kaynak Yavaşlamalı (Source Quench)	Akış kontrol işlevini yerine getirir, kaynak, iletilebilen veriden daha hızlı veri gönderdiğinde yavaşlaması için bu mesaj kullanılır.
Yönlendirme (Redirect)	Yönlendirme ile ağ üzerindeki cihaza seçilebilecek en iyi yol bilgisi verilir.
Yankı (Echo)	Ping komutu ile test işlevini yerine getirir, bağlanırlılığı kontrol etmek için kullanılır.
Parametre Problemi (Parameter Problem)	Parametre sorunu paket başlık parametrelerinde oluşan hataları "parameter problem" mesajı ile geri bildirir.
Zaman Damgası (Timestamp)	Zaman damgası, alıcı kendisine gelen paketin alım için geçen süresini hesaplayıp Time Stamp Reply paketi ile süreyi kaynak düğüme bildirir.
Adres Maske İstemi (Address Mask Request/Reply)	Kullanılacak altağ maskesini (subnet mask) öğrenmek ve hakkında bilgi edinmek için kullanılır. "Address Mask Reply" paketi ile geri gönderilir.

Şekil 2.12: ICMP formatı

Tip 8 bittir, mesaj tipini belirler. Kod, 8 bit kullanır ve mesaj tipi alt gruplarına detaylı tanımlama sağlar. Hata denetimi 16 bit, ICMP mesajının hata denetiminin yapılabilmesi amacıyla kullanılır. Mesaj bağımlı, rezerve edilmiştir. Bilgi alanında IP başlığı kaynak ve hedef adresleri bilgileri yer alır [22, 24].

İnternet Prokotol-IP (Internet Protocol)

Temel olarak datagram paketleri için bir iletim yolu belirleme işlevini yerine getirir. IP'nin sağladığı fonksiyonlar şunlardır:

- Global adresleme yapısı
- Servis isteklerini tiplendirme
- Paketleri iletim için uygun parçalara ayırma
- Hedef alıcıda paketleri tekrar birleştirme

TCP, hedef bilgisi bulunan segmenti IP'ye verir. IP bu segmenti alır herhangi bir diğer datagram veya segmentten önce veya sonra hedef düğüme iletim için bir yol belirler. Her bir datagram veya segment IP tarafından kendi başlığı eklenerek IP paketi haline getirilir ve her bir IP paketi birbirinden bağımsız olarak hedef düğüme gönderilir. Paketler üzerinde çok sınırlı hata kontrolü vardır. IP 16 bitlik başlık hata kontrolü (checksum) sağlar. Bu IP paketini alan düğümün IP başlığında bir bozulma oluşup oluşmadığını kontrol etmesini sağlar. Onay (acknowledge) mekanizması kullanmaz. Verinin internet katmanına bozuk ulaştığını değerlendirip yeniden gönderimi sağlayabilecek fonksiyona sahip değildir. Bu görev bir üst katmandaki TCP'de yapılır, TCP'nin kullanılmadığı durumlarda daha üst katman protokollerince yerine getirilir.

Akış kontrol ve paket sıralama mekanizmalarına sahip değildir. IP bağlantısız paket dağıtım servisi sunar [24].

IP Adresleme

TCP/IP kullanılan ağlarda, adresleme IP adreslere dayanılarak gerçekleştirilir. Ağda bulunan iletişim kuracak her cihaza bir IP adresi atanır, diğer cihazlar bağlantı kurmak için bu adresi kullanır. IP adresleri şu anda yaygın kullanımda olan IP sürüm 4 (IPv4) için 32 bit boyunda olup, noktalarla ayrılmış 4 adet 8 bitlik sayıyla gösterilirler. Ağ katmanında paketler bir noktadan diğer noktaya iletilirken mantıksal adresler kullanırlar. Mantıksal adresler paketin kaynak ve gideceği en son yerin (hedefin) ağ adresini içerir. Adres alanı içinde varış noktasının ağ adresi ile düğüm adresi bileşimi bulunur. Adres uzunluğu 32 bittir. 2^{32} adet IP adresi içerir, bu durumda 4.294.967.296 bilgisayar internete bağlanabilir. IP adresleri, bilgisayar ağlarını bölümlemek ve farklı büyüklüklerde bilgisayar ağları oluşmak üzere sınıflandırılmıştır. IP, 5 farklı adres formatını destekler, bunlar; A, B, C, D ve E sınıfı adreslerdir. Her adres sınıfı o adresi tanımlayan ilk baytın en anlamlı bitlerine yerleşen bir bit dizisi ile tanımlanır. Bu bit dizisini A, B, C sınıfı adreslerde ağ adresi ve sonrasında düğüm adresi takip eder [9, 14, 24].

A sınıfı adreslerde ilk bayt ağı tanımlamak için kullanılır. İlk bit 0'dır. Ondan sonraki 7 bit ağ adresini oluşturur. Geri kalan 24 bit ağdaki host (makine) sayısını belirler. 2^{24}-2 ile herbiri 16.777.214 adet bilgisayar içeren 126 adet altağ (subnet) kullanılabilir. Host bitlerinin tamamı 1 olan adresler yayın (broadcast) ve 0 olanlar ise ağ adresi olarak kullanılır.2^{7}-2 ile 126 olan altağ sayısı hesaplanır. 0.0.0.0 adresi varsayılan yönlendirme 127.0.0.0 adresi ise yerel çevrim için kullanılır [14]. İlk sekizli aralığı 1–126, geçerli ağ numaraları 1.0.0.0 – 126.0.0.0'dır [6].

B sınıfı adreslerde ilk iki bayt, ağı tanımlar. İlk iki bit adres sınıfını belirler, 1 ve 0 şeklindedir. Diğer 14 bit ağ adresini oluşturur, sonraki 16 bit ağdaki host sayısını belirler. Her biri 65.534 olmak üzere 16.384 adet altağa izin verir. 128.0.0.0 ve 191.254.0.0 adres aralığını kullanılır [6].

C sınıfı adreslerde ilk üç bayt ağı tanımlar. İlk üç bit(110) adres sınıfını belirler ve diğer 21 bit ağ adresini oluşturur. Kalan 8 bit ağdaki host sayısını belirler. 254 adet bilgisayar içeren 2.097.152 altağa izin verilir. 192.0.1.0 ve 223.255.254.0 aralığı kullanılır [6, 14].

D sınıfı adresler multicast adresleme için kullanılır. İlk dört biti 1110 şeklindedir. 224.0.0.0 – 239.255.255.255 adresleri kullanılır.

E sınıfı adresleme yedek olarak saklı tutulmaktadır. İlk dört biti 1111 şeklindedir.

Yerel ağlarda kullanılmak üzere 10.0.0.0, 172.0.0.0 ve 192.168.0.0 ağ adresleri saklı tutulmuştur [14].

IP adreslemesi IPv4 standartlarına göre yapılmakta, IP adresleri 32 bitten oluşmaktadır fakat bu IP adreslerinin tamamı tükenmek üzere olduğunda IP adresleri IPv6 standartlarına göre verilmeye başlanacaktır. Bu adresleme tekniğinde IP adresleri 32 değil 128 bitten oluşmaktadır [24].

2.4.4. Fiziksel Katman

Fiziksel katman, veri bağı ve fiziksel ortamı içermektedir [4]. OSI referans modelindeki birinci ve ikinci katmanların görevlerini yerine getirir. Fiziksel katman için bir protokol tanımlanmamıştır. Ethernet bağlantısı, modem üzerinden çevrimiçi bağlantı ve varolan fiziksel bağlantı türlerini kullanmaktadır. Uç sistemde TCP/IP modülünün çalışması yeterlidir [14].

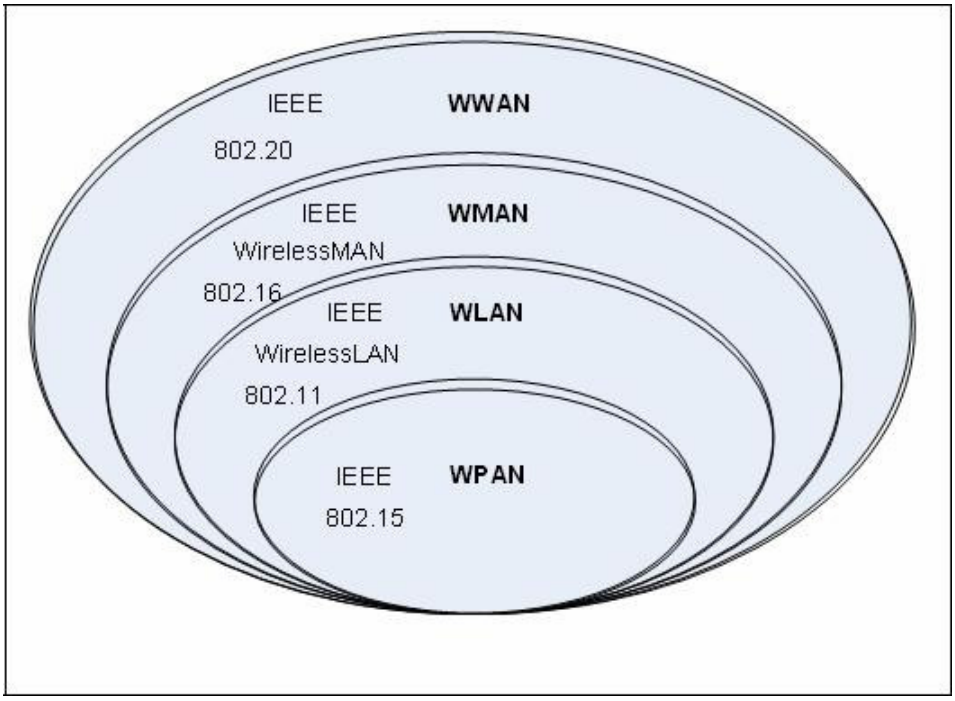
3. KABLOSUZ AĞLAR

Kablosuz genel bir terimdir, bir noktadan başka bir noktaya bakır kablo gibi fiziksel bir bağlantı kullanmadan yapılan veri, ses veya görüntü taşımaya denir [25]. Kablosuz ağ teknolojileri, kullanıcılara uzak mesafeler arasında kablosuz bağlantılar kurmalarına izin veren küresel ses ve veri ağlarından, kısa mesafelerde kablosuz bağlantı için en iyi hale getirilmiş kızılötesi ışınlar ve radyo frekans teknolojilerine kadar uzanmaktadır. Genelde kablosuz ağlarda kullanılan aygıtlar, taşınabilir bilgisayar, masaüstü bilgisayarı, el bilgisayarı, kişisel dijital yardımcı (PDA-Personal Digital Assistant), cep telefonu, kalemli bilgisayar ve çağrı cihazlarını kapsamaktadır. Kablosuz teknolojiler birçok kolaylık sağlar. Örneğin cep telefonu kullanıcıları, e-postalarına erişmek için cep telefonlarını kullanabilirler. Taşınabilir bilgisayarlarla seyahat edenler, hava alanlarında, tren istasyonlarında ve diğer genel noktalarda kurulu baz istasyonları aracılığıyla internete bağlanabilirler. Evdeki kullanıcılarsa, veri eşitleme ve dosya aktarımı için masaüstlerindeki aygıtlara bağlanabilirler [26].

Kablosuz ağlar, kablo limiti olmaksızın geleneksel ağ teknolojilerinin bütün imkân ve avantajlarını sağlar. Kablosuz sistemler tamamen kablosuz değildir. Bu sistemler geleneksel ağlara bağlanmak üzere, standart mikroişlemciler ve sayısal devreler kullanırlar. Kablosuz aygıtlar, kodlama, sıkıştırma, taşıma ve sinyal alma işlemleri için geliştirilmektedirler [27]. Kablosuz ağlar, pahalı fiber kaplama ve kablo döşemenin yüksek maliyetini düşürür veya ortadan kaldırır ve kablolu ağlara yedekleme işlevselliği sağlar. Kablosuz ağlarla aygıtların uyumlu, ekonomik ve güvenli olduğundan emin olmak üzere, şirketler ve özel yatırımcı gruplar, kablosuz iletişimin standartlarını geliştirmek için çalışmaktadır [26].

3.1 KABLOSUZ AĞ TÜRLERİ

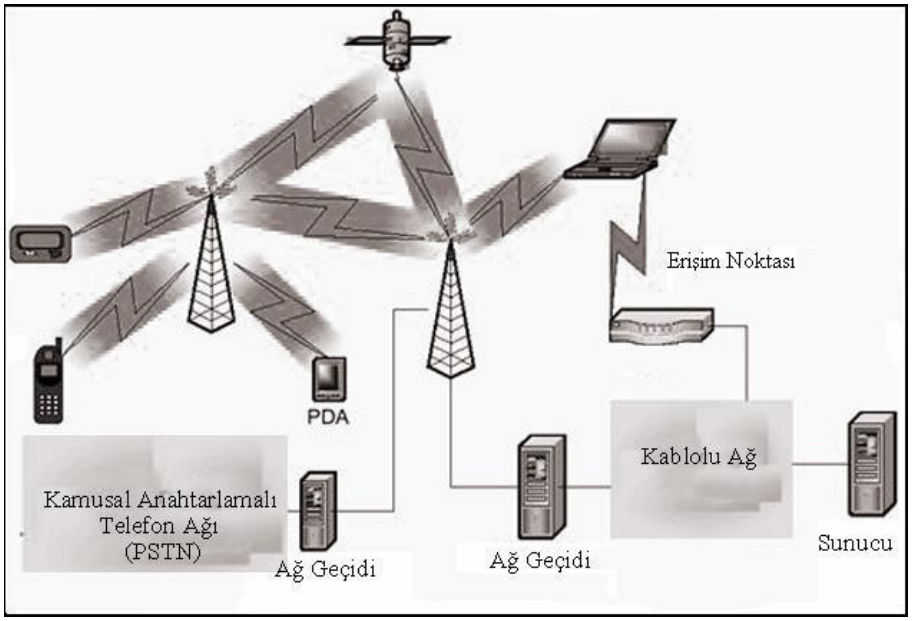
Kablosuz ağlar kullanım amaçları ve yapılarına göre sınıflandırılmıştır. Sınıflandırma çerçevesinde standartlar oluşturulmuştur.



Şekil 3.1: Kablosuz ağ standartları

3.1.1. Kablosuz Geniş Alan Ağları (WWAN-Wireless Wide Area Network)

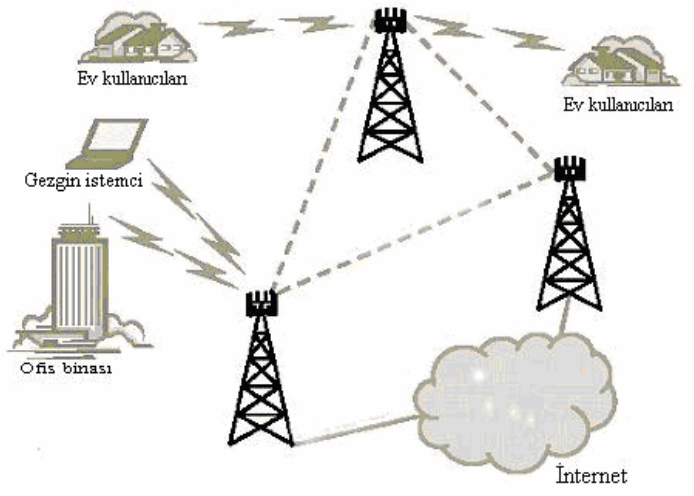
WWAN teknolojileri, kullanıcıların, uzak ortak veya özel ağlar üzerinden kablosuz bağlantı kurmalarına olanak tanır. Bu bağlantılar, kablosuz hizmet sağlayıcılarının sunduğu birden çok anten istasyonu ve uydu sistemi kullanımı aracılığıyla, çok sayıda şehri ve ülkeyi içine alan geniş coğrafi bölgeleri kapsayabilir. Şu andaki WWAN teknolojileri, ikinci kuşak (2G) sistemler olarak tanınmaktadır. Temel 2G sistemleri, Gezgin İletişim için Küresel Sistem (GSM-Global System for Mobile Communications), Hücresel Sayısal Paket Veri (CDPD-Cellular Digital Packet Data) ve Kod Bölüşümlü Çoklu Erişim (CDMA-Code Division Multiple Access) sistemlerini kapsamaktadır [26].



Şekil 3.2: Kablosuz geniş alan ağları

3.1.2. Kablosuz Anakent Alanı Ağları (WMAN-Wireless Metropolitan Area Network)

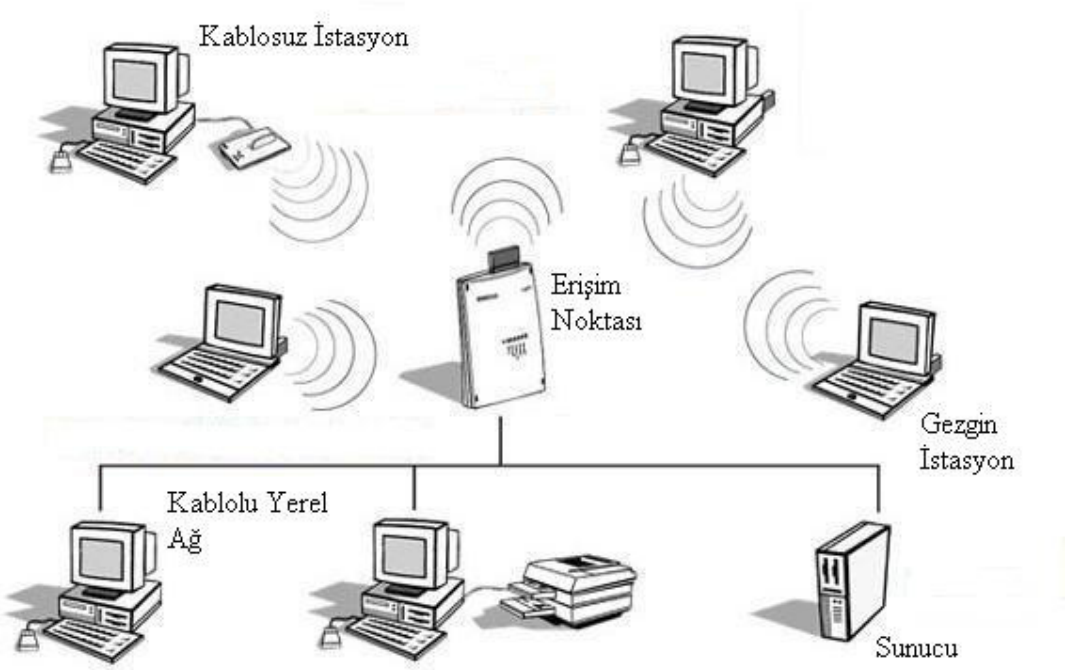
WMAN teknolojileri, kullanıcılara anakent alanı içinde çeşitli yerler arasında kablosuz bağlantılar kurma olanağı verir. Buna ek olarak, WMAN'ler, kablolu ağların birincil kiralanmış hatları kullanılabilir olmadığında yedek olarak da hizmet verebilir. WMAN'ler veri aktarımı için radyo dalgaları veya kızılötesi ışınlar kullanır [26] .



Şekil 3.3: Kablosuz anakent alanı ağları

3.1.3. Kablosuz Yerel Alan Ağları (WLAN-Wireless Local Area Network)

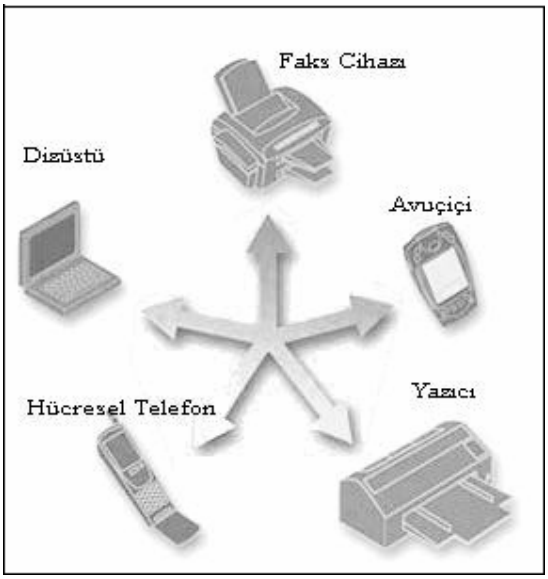
WLAN teknolojileri, kullanıcıların yerel alan içinde (şirket, kampüs binası ve havaalanı gibi bir ortak alanda) kablosuz bağlantı kurmalarına olanak sağlar. WLAN'ler, çok sayıda kablo bağlamanın engelleyici olacağı geçici ofislerde veya diğer alanlarda kullanılabileceği gibi, kullanıcıların bina içinde farklı yerlerde ve farklı zamanlarda çalışabilmeleri için varolan bir yerel ağı tamamlamak için de kullanılabilir [26].



Şekil 3.4: Kablosuz yerel alan ağları

3.1.4. Kablosuz Kişisel Alan Ağları (WPAN-Wireless Personel Area Netwok)

WPAN teknolojileri kullanıcılara kişisel işletim alanı içinde kullanılacak (PDA, cep telefonu veya dizüstü bilgisayarları gibi) aygıtlar için özel, kablosuz iletişim kurma olanağı tanır. Kişiyi 10 metre uzaklığa kadar çevreleyen bir alandır. Şu andaki iki temel WPAN teknolojisi Bluetooth ve kızılötesi ışındır. Bluetooth, 10 metrelik uzaklığa kadar veri aktarmak için kablo yerine radyo dalgaları kullanan bir teknolojidir. Bunun yanı sıra, kullanıcılar aygıtlar arasında çok kısa mesafelerde (1 metre veya daha az) bağlantı kurmak için kızılötesi bağlantılar oluşturabilir [26].



Şekil 3.5: Kablosuz kişisel alan ağları

3.2. KABLOSUZ YEREL AĞ STANDARTLARI

İlk kuşak WLAN aygıtları düşük hızları, standart eksikleri ve yüksek maliyetleri ile kullanışlı değildi. Toplam bant genişliğinin 1-2 Mbps gibi bir hızla kısıtlı olması, farklı firmalar tarafından üretilen ağ arayüz kartı (NIC-Network Interface Card) ve erişim noktalarının (AP-Access Point) birbirleri ile uyumlu çalışamama probleminden dolayı tercih edilmiyordu. Ethernete benzer standartlara ihtiyaç duyulduğunda kablosuz üreticileri 1991'de birleştiler ve Kablosuz Ethernet Uyumluluk Birliği'ni' (WECA-Wireless Ethernet Compatibility Allience) kurdular. WECA istenilen teknoloji üzerinde temel standart oluşturdu. Daha sonra adını Wi-fi olarak değiştirdi. Wi-fi, Kablosuz Sadakat Birliği'nin (Wireless Fidelity Alliance) tescilli markasıdır. Wi-fi Alliance küresel, karsız endüstri kuruluşudur. Haziran 1997'de IEEE 802.11 standardını çıkardı. 802.11 standardına uygun çıkarılan ürünler ülkemizde lisanssız olarak kullanılabilen bir bant olan 2.4 Ghz'de çalışmakta ve 1 Mbsp'den 2 Mbps'e varan paylaşımlı veri transfer hızına erişebilmektedir. Wi-Fi sertifikasyonu ile farklı firmaların ürünleri arasındaki uyumsuz çalışma problemi halledilmiş oldu. Böylece kablosuz yerel alan ağları günümüzdeki popülaritesini kazandı. Bugün Wi-Fi kablosuz ağlar için genel bir ifade olarak yaygın şekilde kullanılmaktadır. Modern standartlaşmış sistemler, kabul edilebilir hızlarda veri transferi yapabilmektedir [25, 27, 28].

Kablosuz bilgisayar ağı cihazları, ilk olarak askeri ihtiyaçlar için geliştirilen, daha sonraları sivil amaçlarla kullanılmaya başlayan yayılı spektrum (spread spectrum) tekniğini kullanır. 3 tip yayılı spektrum teknolojisi vardır;

Doğrudan Sıralı Yayılı Spektrumu (DSSS-Direct Sequence Spread Spectrum)

Radyo frekans (RF) sinyalinin geniş bir bant aralığına oturtulması ve bu aralığa yayılmış olan sinyalin verici-alıcı cihazlar tarafından işlenmesi teknolojisidir. Yayılı spektrum üzerinde doğrudan diziyle yayma (direct sequence) modülasyonu kullanmaktadır. Cihazlar 2.4 - 2.5 Ghz frekansını kullanmaktadır [29, 27].

Frekans Atlamalı Geniş Spektrum (FHSS Frequency-Hopping Spread Spectrum)

Geniş spektrum modülasyon şemasıdır, alıcı ve verici cihazın bildiği bir şablon çerçevesinde bir dar bant taşıyıcı ile frekansı değiştirmektedir. Doğru senkronizasyon ile tek bir mantıksal kanal oluşturulur. Haberleşme için senkronizasyon yapmamış bir alıcı cihaz tarafından FHSS kısa süreli bir gürültü darbesi şeklinde yorumlanır. Veri çok küçük paketlere bölünerek diğer cihaza rastgele değişen frekanslarda (toplam 79 frekans) gönderilir. Sadece önceden anlaşma sağlanan şablon frekansında senkronize olmuş alıcı-verici cihazlar bu verileri alıp, gönderebilirler. Gönderen cihaz saniyede 1,600 kez frekans değiştirerek yüksek seviyeli bir güvenlik sağlar [30].

Dikey Frekans Bölüşümlü Çoğullama (OFDM-Orthogonal Frequency Division Multiplexing)

OFDM radyo dalgaları üzerinden büyük miktarda veri transferi yapmak için kullanılan bir frekans bölüşümlü çoğullama modülasyon tekniğidir. OFDM radyo sinyalini daha küçük alt sinyallere bölüp aynı anda farklı frekanslardan alıcıya gönderme yöntemi ile çalışır. OFDM sinyal iletiminde meydana gelen çapraz karışmayı azaltan ve çoklu-yol gecikme yayılmasına ve kanal gürültüsüne tolerans tanıyan bir yöntemdir. Bu yüzden pek çok kablosuz uygulama için oldukça uygundur [27, 28].

Taşıyıcı Algılaması Çoklu Erişim/Çakışma Kaçınma (CSMA/CA-Carrier Sense Multiple Access/Collision Avoidance)

Ağdaki çarpışmaların önüne geçebilmek için kullanılan ağ bağlantı protokolüdür. Kablosuz ağ trafiğini sağlar. CSMA/CA gerçek veri dağıtımı yapılmadan önce çarpışmaları dinlemek için ağa bir sinyal gönderir, çarpışma duyduğunda, WLAN üzerindeki diğer aygıtlara hiçbir veri yayınlamamalarını söyler [25].

IEEE 802.11 iletim şekli ve iletim ortamını tanımladığı için OSI'nin birinci ve ikinci katmanında faaliyet göstermektedir. Modülasyon şekilleri olan DSSS, FHSS, OFDM OSI'nin fiziksel katmanı ile ilgilidir. Diğer güvenlik ve iletim ile ilgili kısımlar ikinci katmanda (veri bağı) işlenir [31].

3.2.1. IEEE 802.11 Standartları

IEEE tarafından standartları belirlenen 802.11 kablosuz iletişim protokolü zaman içerisinde bazı değişikliklere uğramıştır. Yaygın olarak kullanılan 802.11 standartları şu şekildedir;

IEEE 802.11b: Eylül 1999 yılında standart olmuştur. DSSS 2.4Ghz spektrumunu kullanır. Bu spektrum aynı zamanda kablosuz telefon ve çoğu bluetooth ürünleri tarafından da kullanılmaktadır. Maksimum 11Mbit bant genişliği sağlar. Kapsama alanı kapalı alanlarda 30–45 metredir.

IEEE 802.11a: 5Ghz radyo bandında en fazla 54Mbit bant genişliği sağlar. OFDM teknolojisini kullanır. 802.11b ve 802.11g standartlarıyla uyumsuzdur.

IEEE 802.11g: 2.4Ghz spektrumunu kullanır. Maksimum bant genişliği 54Mbit. 802.11b ürünleriyle uyumludur.

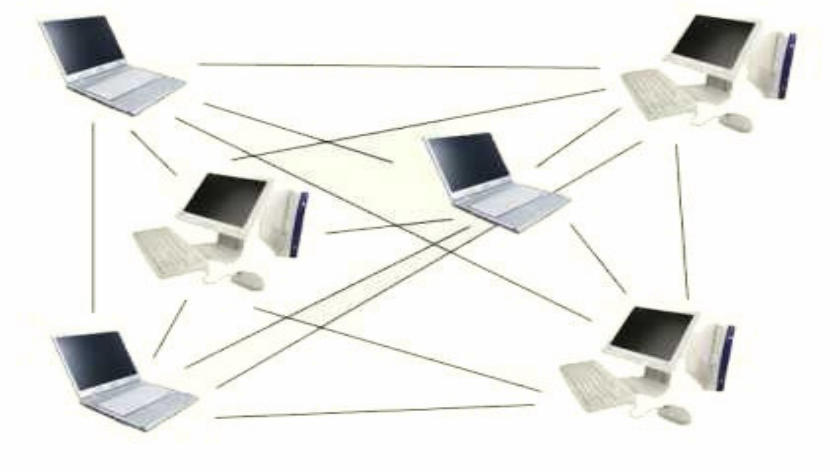
IEEE 802.11i: Kablosuz ağların güvenlik problemlerine detaylı çözümler üretmesi amacıyla geliştirilmiştir [32, 33].

IEEE 802.11n: Şu anda taslak aşamasında 802.11n standardı, maksimum veri transfer hızını 540 Mbps çıkarmaya, bunun yanında eş zamanlı olarak çoklu veri iletişimi yapılmasına imkân tanıyan yeni standarttır.

Kablosuz ağlar yapılanma şekillerine göre altyapısız ağlar ve altyapılı kablosuz ağlar olarak iki kısımda çalışmaktadır.

3.2.2. Altyapısız (Tasarsız) Ağlar

Bağımsız Temel Hizmet Seti (IBSS-Independed Basic Service Set) olarak da bilinir. Tasarsız ağlar çok adımlı, altyapısız ve genellikle hareketli düğümlerden oluşan kablosuz ağlardır. Bu ağlarda düğümler hem diğer düğümlerle iletişim kurarlar hem de paketleri ileterek yönlendirici görevi görürler. Tasarsız ağlar askeri, arama kurtarma, konferans salonu, ofis, kampüs, üniversite ve şehir ağlarında kullanılmaktadırlar. Tasarsız ağlarda bir altyapının mevcut olmaması, düğümlerin hareketli olması, güç kapasitesinin ve bant genişliğinin kısıtlı olması bu ağların en büyük problemleridir. Özellikle düğümlerin hareketliliği topolojinin sık değişmesine ve kurulan yolların bozulmasına neden olmaktadır [34, 35].



Şekil 3.6: Tasarsız ağlar

3.2.3. Altyapılı Kablosuz Ağlar

Temel Hizmet Seti (BSS-Basic Service Set) adı verilen birden fazla istemcinin bir ana istasyon üzerinden bağlandığı yöntemdir. Bu bağlantı şekline erişim noktalı bağlantı veya noktadan çok noktaya bağlantı denmektedir. Bu yöntemde bütün trafik erişim

noktası Erişim noktasından geçer. Altyapı olarak bir erişim noktası kullanırlar, bu aygıt ile ağa bağlanarak birbirleriyle iletişim kurarlar [34, 35].

Şekil 3.7: Altyapılı kablosuz ağlar

3.3. KABLOSUZ AĞLARDA GÜVENLİK

Kablosuz ağlarla ilgili çalışmaların hız kazanmasıyla, kablosuz ağların kullanımı artmış, oluşturulan yeni standartlar kullanımı kolaylaşmıştır. Kablosuz ağlar, kablolu ağların birtakım fiziksel problemlerini ortadan kalkmakta ve ağa dahil olmak isteyen hareketli cihazların kolayca bağlanabilmesini sağlamaktadır. Fakat iletişim radyo dalgaları aracılığıyla korumasız hava ortamında gerçekleştiği için, paylaşılan verilerin güvenliği çok önemli bir konuma gelmiştir. Kullanımın artması beraberinde güvenlik problemlerini doğurmuştur. Kablosuz ağlarda güvenlik, kablosuz ağlarla ilgili yaşanan sorunların başında gelmektedir [36].

Ağ güvenliği, korunmuş dijital bilgi varlıkları sürecidir. Güvenlik hedefleri, bütünlüğü devam ettirmek, gizliliği korumak ve varlığından emin olmaktır. Öncelikli güvenlik beklentisi, varlıkları, ağın devamlığını ve iş süreçlerini korumaktır. Birçok kişi için bu, güçlü duvarlar inşa etmek ve seçilen bir grup insan için emniyetli giriş sağlamaya yönelik iyi korunmuş kapılar oluşturmak anlamındadır. Bu strateji kablosuz ağlardan daha çok kablolu ağlar için uygun bir çalışmadır. Tek bir güvenlik duvarı kablosuz ağ güvenliği sağlamak için çok uygun değildir, çünkü kablosuz sinyalleri fiziksel olarak

izole etmek zordur. Emniyetli kablosuz ağlar için ilave teknolojiler ve stratejiler kullanılmak zorundadır.

Güvenlik, kullanıcıların sadece yapmaya yetkili oldukları görevleri ve yalnız yetkiye sahip oldukları bilgileri içerebilen bilgilere ulaşması değil, aynı zamanda kullanıcının sistem verilerine, uygulamalarına ve işletim sistemine zarar verememesinden emin olmaktır. Güvenlik, aynı zamanda ekipman özellikleri ve hata etkilerini kontrol eden program saldırılarına karşı korumayı içerir. Kablosuz ağ güvenliği kısmi güvenlik mücadelelerini ifade eder. Kablosuz ağlarda güvenlik protokolleri yönetimi erişim, performans, kullanım kolaylığı, yönetim, kullanışlılık ile doğrulama (Authentication), yetkilendirme (Authorization), hesap yönetimi (Accounting), güvence, gizlilik ve veri bütünlüğü arasında dengeleme sağlamalıdır [27]. Doğrulama, kablosuz ağa bağlanmak isteyen kullanıcı ya da cihazın kimliğini gösterir. Yetkilendirme, doğrulanan bu kullanıcı ya da cihazın kablosuz ağa erişim için izni olup olmadığını gösterir [37].

3.3.1. Kablosuz Ağ Tehditleri

Kablosuz teknolojiler tamamıyla emniyetli olsaydı WLAN tehditleri endişe kaynağı olmayacaktı. Bununla birlikte birçok bilinen ve bilinmeyen açıkların varlığı ile saldırganlar yüksek bir tehdit yarattı. Kablosuz güvenlik tehditleri için öncelikli dört sınıf vardır:

- Yapılandırılmamış tehditler
- Yapılandırılmış tehditler
- Harici tehditler
- İç tehditler

3.3.1.1. Yapılandırılmamış Tehditler

Çoğunlukla kolaylıkla ulaşılabilen korsan araçlarını, kabuk komut dosyaları (shell script) gibi, ağ keşif (war driving) programları ve şifre kırıcıları kullanan deneyimsiz bireylerden oluşur.

3.3.1.2. Yapılandırılmış Tehditler

Yüksek istekli ve teknoloji yetenekli saldırganlar tarafından gelir. Bu insanlar kablosuz sistemin derin açıklarını bilir ve sömürü kodları (exploit-code) gelişimini, scriptleri ve programları anlayabilirler. Bildiklerini ve araçları diğerleriyle paylaşırlar.

3.3.1.3. Harici Tehditler

Kişisel veya şirket dışından organize çalışmalardır. Kablosuz ağa izinli giriş yapmazlar, ağ içinde çoğunlukla yapının dışından, park alanlarından, komşu binalardan veya yaygın alanlardan kendi yöntemleriyle çalışırlar. Harici tehditler, insanların çok zaman harcayıp kazanç sağladığı tehditlerin bir tipidir.

3.3.1.4. İç Tehditler

Bir sunucu üzerinden hesabıyla yetkili giriş yaptığı zaman veya fiziksel, kablolu giriş yaptığı zaman oluşur. Resmi kayıtlara göre %60 ila %80 oranındaki raporlanmış olaylar iç girişler ve kötüye kullanılmış hesaplardır. Zayıf kablosuz sinyaller ile ağın fiziksel sınırsızlığı dışında, WLAN şimdi harici ataklara karşı kolaylıkla elde edilebilir. Kablosuz girişler ağ güvenliğine son derece büyük tehdit olabilir. Erişim noktasıyla irtibat kurduğunda saldırgan iç ağa kolaylıkla girip dolaşabilir [27].

3.3.2. Mevcut Güvenlik Yöntemleri ve Protokolleri

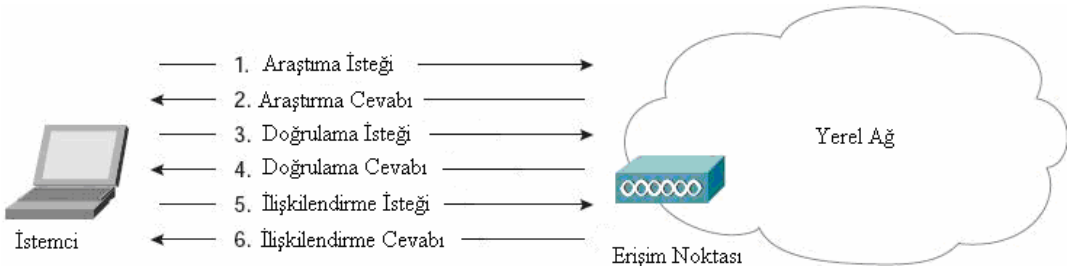
Kablosuz ağların ilk yıllarında güvenlik büyük bir kaygı değildi. Donanımlar şirkete özel pahalı ve bulması zordu. Kablosuz ağların yaygınlaşmasıyla güvenlik amaçlı yapılan çalışmalar, kablosuz ağlarda saldırıların artık kolay olmadığını göstermiştir. Bu güvenlik çalışmaları çerçevesinde çeşitli şifreleme algoritmaları geliştirilmiş, yetersiz algoritmaların yerini daha kuvvetli algoritmalar almıştır.

3.3.2.1. Servis Seti Tanımlayıcı (SSID-Service Set Identifier)

Servis seti tanımlayıcı (SSID), kablosuz ağın mantıksal adıdır. Kablosuz ağa bağlanması olası kablosuz cihazlara ağın kimliğini verir. SSID, istemci ve erişim noktalarına girilebilen 1'den 32'ye kadar ASCII dizgidir. 802.11 altında boş dizgili herhangi bir istemci erişim noktasındaki SSID ayarlarından bağımsız olarak herhangi

bir erişim noktasına birleşir. Bazı erişim noktaları SSID yayınlama ve herhangi bir SSID'ye izin verme gibi seçeneklere sahiptir. Herhangi bir SSID seçeneğini kullanmak erişim noktasının boş SSID'li bir isteminin erişimine izin verir. İlk kuşak kablosuz ağlar SSID'yi güvenliğin temel şekli olarak kullanmışlardır [25, 27].

İstemci erişim noktası bulmak için üye edildiği SSID'yi sorgulayabilir. Giriş noktası belirlendikten sonra istemci karşılıklı doğrulamayı yerine getirmek zorundadır. Başarılı bir doğrulamadan sonra istemci doğrulanmış, ilişkilendirilmemiş olan ikinci adıma gider. Bu durumu da geçen istemci son duruma gelir ve son ilişkilendirilmiş ve doğrulanmış durumunda bir ortaklık mesajı gönderir ve giriş noktası yanıtı ortaklığı kurar. Yukarıda anlatılanlar gerçekleştikten sonra istemci kablosuz ağda eş konumuna gelir ve ağda veri yayınlayabilir Durumlar arası geçiş, yönetim çerçeveleri (management frames) mesajları ile gerçekleşir [38].



Şekil 3.8: 802.11 istemci doğrulama süreci

Zayıflıkları

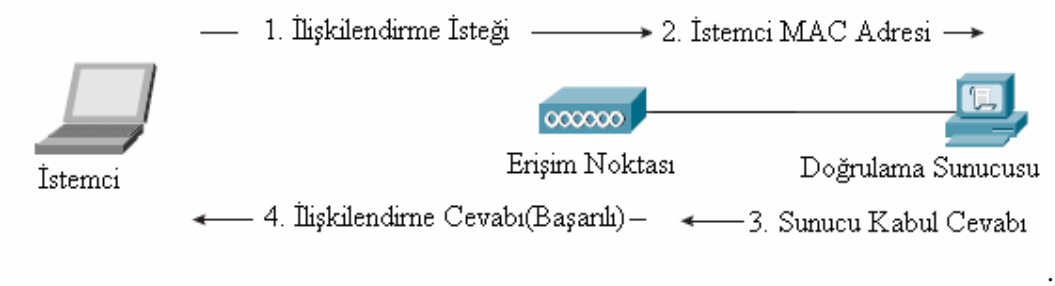
SSID yayınlama seçeneği SSID'yi tanımlayan işaret çerçevesi (beacon frame) gönderir. Bu seçeneği kapatmak ağı güvenli hale getirmez çünkü bir kablosuz ağ dinleyicisi (sniffer) araştırma istekleri, araştırma istek yanıtları ve bağlantı isteklerini dinleyerek kolayca normal WLAN trafiğinden geçerli bir SSID'yi ele geçirebilir, aynı SSID ile yayın yaparak istemcileri kendi erişim noktasına yönlendirebilir. SSID'ler bir güvenlik özelliği olarak kabul edilmemeliler [25, 27, 38]

3.3.2.2. MAC Adresi ile Doğrulama

MAC tabanlı doğrulama 802.11 standardında tanımlanmamıştır. Bununla birlikte birçok tedarikçi MAC tabanlı doğrulamayı uyarlamıştır. Tedarikçilerin çoğu basitçe, her erişim

noktasının geçerli bir erişim kontrol listesi olmasına ihtiyaç duyarlar. Bazı tedarikçiler erişim noktasının merkezi sunucu üzerindeki MAC adres listesini sorgulamasına izin verirler. Erişim kontrol listeleri, kullanıcının sahip olduğu kablosuz ağ kartındaki MAC adreslerine göre yapılır. AP'ler, kullanıcının ağı kullanmasını bu erişim kontrol listelerine göre sınırlandırırlar. Eğer kullanıcının MAC adresi listede varsa ve ağa ulaşım için izin verilmişse ağ kaynaklarına erişime izin verilir. Farklı durumda erişim engellenecektir.

1) Kullanıcı Erişim noktasına doğrulama isteği gönderir.
2) Erişim noktası, kullanıcının MAC adresini doğrulama sunucusuna gönderir.
3) Sunucu kabul ya da ret cevabını erişim noktasına gönderir.
4) Erişim noktası kullanıcıyı doğrular.



Şekil 3.9: MAC adresi ile doğrulama

Zayıflıkları

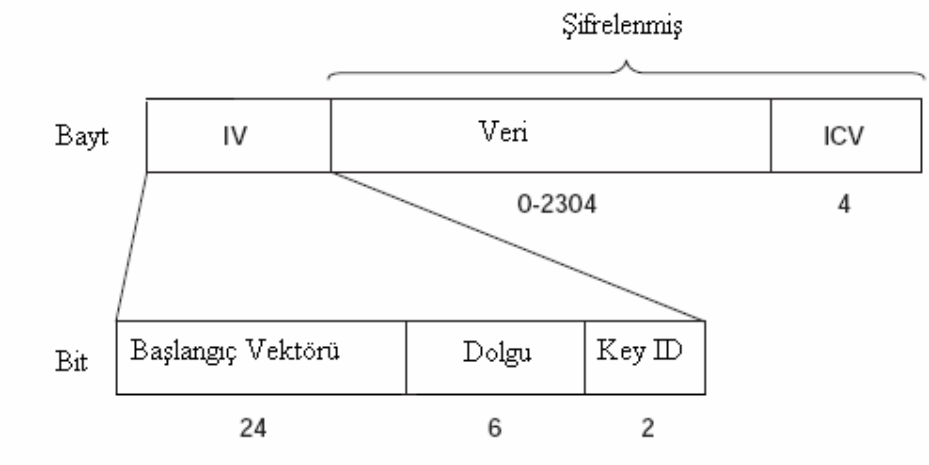
Kablosuz ağ erişimini, MAC adresleri kullanarak kontrol etmek takibi zor bir iştir. Hassas envanter tutulmalı ve kullanıcılar kayıp ve çalıntı ekipmanı hemen rapor etmelilerdir. MAC adresleri gerçek bir güvenlik mekanizması değildir çünkü tüm MAC adresleri iletilirken şifresizdir. Bir saldırgan MAC aldatma (spoofing) olarak isimlendirilen bir tekniği kullanarak ağa ulaşabilmek için sadece geçerli bir MAC adresi elde etmesi gereklidir. Saldırgan bir dinleme programı kullanarak ağ trafiğini yakalar, sonra yetkili MAC adresi için trafiği analiz eder, sonrada kendi MAC adresini güvenilir MAC adresi ile değiştirir. MAC adresi değiştirme basit bir kayıt değişimidir. Birçok yardımcı program ile kolaylıkla yapılabilir. Belirli durumlarda MAC adres doğrulaması güvenlik özelliklerinin eksiklerini giderebilir, fakat bu hiçbir zaman kablosuz güvenlik sağlamanın ana metodu olmamalıdır [25, 27].

3.3.2.3. Kabloluya Eşdeğer Gizlilik (WEP-Wired Equivalent Privacy)

WEP, 802.11 standardıyla beraber geliştirilmiş olan temel güvenlik birimidir. WEP'in tasarlanmasının üç önemli amacı bulunmaktadır ve bunlar güvenilirlik, erişim kontrolü ve veri bütünlüğüdür.

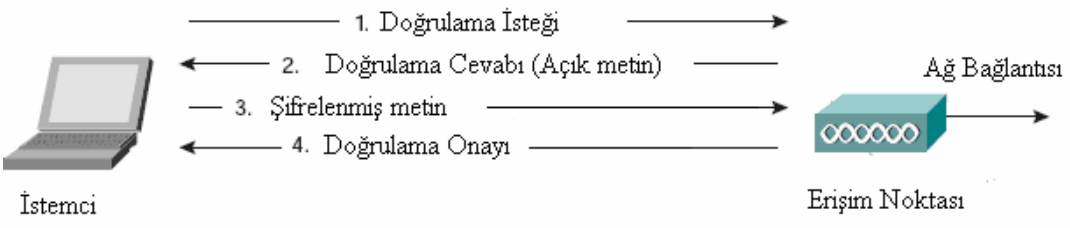
WEP'in teknik altyapısı Ron Rivest tarafından bulunan RC4 (Rivest Cipher) akış şifreleme algoritmasına dayanır. RC4'ün amacı, verilen bir gizli anahtar ile geniş uzunlukta rasgele sayılar üretmek ve daha sonra bu akışla göndericide düz metin mesajı şifrelemektir. Alıcı, verilen anahtarla aynı akışı üretebilecek ve alınan mesajın şifresi çözülebilecektir. Mesajın şifrelemesinin çözümlenmesi ve şifrelemesi temel olarak dar veya (XOR) fonksiyonu ile yapılmaktadır [36]. WEP şifreleme ve şifre çözme şu şekilde çalışmaktadır;

24 bitlik başlangıç vektörü (IV-Initialization Vector), 40 bitlik paylaşılan anahtara eklenir. Bu anahtardan RC4 algoritması kullanılarak şifrelenecek veri uzunluğunda akış şifresi elde edilir. IV vektörünün değişmesi ile her seferinde farklı akış şifreleri elde edilmektedir. Bu sırada veri bütünlüğü sağlamak için asıl veri üzerinden bütünlük kontrol değeri (ICV-Integrity Check Value) hesaplanır ve verinin sonuna eklenir. Elde edilen akış şifresi ile (veri +ICV) dar veya işleminden geçirilerek şifreli metin hazırlanmış olur. Son adım olarak alıcı tarafın şifreyi çözmesi için bilmesi gerekli olan IV çerçevenin başına şifrelenmeden eklenir. Böylelikle gönderilecek çerçeve hazırlanmış olur. Şifre çözmede ise alıcı taraf IV'yi çerçeveden okur anahtar kendinde olduğu için akış şifresini elde edebilir. Şifreleme işlemlerini ters sıra ile gerçekleştirerek açık veriyi elde eder [39, 40].



Şekil 3.10: WEP çerçeve yapısı

İstemci bağlanmak istediği erişim noktasını seçtiğinde erişim noktası tarafından istemciye şifresiz bir sorgu paketi gönderilir. İstemci gelen bu sorgu paketini WEP anahtar ile şifreler ve erişim noktasına geri gönderir. Erişim noktası gelen paketin doğru WEP anahtarı ile şifrelendiğini kontrol eder. Doğru WEP anahtar kullanılmışsa erişim noktası istemcinin kendisine üye olmasına ve veri göndermesine izin verir [41].



Şekil 3.11: Anahtar paylaşımlı doğrulama süreci

WEP'te anahtar yönetim mekanizması yoktur. Ortak anahtarın, kullanıcılar tarafından bilindiği varsayılır. IEEE 802.11 standardı, anahtarın önceden paylaşıldığını kabul eder [42].

Zayıflıkları

Doğrulatma: Ağı dinleyen saldırgan, erişim noktasından açık metin ve istemciden şifrelenmiş metni elde edebilir. Açık metin ve şifrelenmiş metni dar veya işlemi

uyguladığında anahtar dizesini elde edebilir ve bununla doğrulama işlemi gerçekleştirebilir.

Tekrar Saldırıları: WEP'te tekrar saldırıları için herhangi bir güvenlik önlemi yoktur. Aynı mesaj defalarca gönderilebilir ve bu alıcı tarafından anlaşılamaz. Sisteme giriş yapan bir kullanıcı sistemden çıktıktan sonra dinlenilen mesajlar doğrulayıcıya gönderilirse araya giren kişi, mesaj içeriğini bilmese de kendini doğrulatabilir.

Bit Değiştirme: ICV bütünlük kontrol verisinin oluşturulma şeklinden kaynaklanmaktadır. ICV lineer bir metotla oluşturulup asıl verinin sonuna eklenip şifrelenmektedir. Lineer bir metotla oluşturulduğu için şifreli olsa bile veri alanında bir değişiklik yapıldığında ICV de oluşacak değişiklik hesaplanabilmektedir.

1) Saldırgan dinlediği ağdan bir paket alır.
2) Dinlediği paketteki veri ve ICV alanlarını değiştirir.
3) Bu paketi ağa gönderir.
4) Erişim noktası ICV değerini kontrol edip çerçeveyi 3. katmana gönderir.
5) 3. katmanda CRC kontrol edilir ve belirli edilen bir hata döndürülür.
6) Erişim noktası bu hatayı şifreler ve gönderir.
7) Araya giren belirli hatanın hem şifreli hem de açık metnine sahip olur. Dar veya işlemi ile buradan akış şifresi elde edilir [41].

IV'lerin Tekrar Kullanılması: IV 24 bittir, 2^{24}'den yaklaşık olarak 17 milyon farklı IV oluşabilir. Tekrarlanmadan birer artırarak kullanıldığında 802.11b standardına göre yaklaşık 7 saatte tüm IV'ler kullanılmış olacaktır. Dar veya işlemi ve dilin yapısal özelliklerinde faydalanarak akış şifresi parça parça elde edilebilir ve akış şifresi çözüldükten sonra bu IV ile sahte çerçeveler oluşturulabilir [39]. Elde edilen akış şifresi ile şifrelenmiş mesajlar analiz yöntemleri kullanılarak açık metin elde edilebilir.

RC4 Zayıf Anahtarlar Üretmesi: RC4 algoritmasının anahtar üretim algoritması (key scheduling algorithm) zayıf akış anahtarları üretmektedir. Bu zayıflıktan faydalanarak şifrelenmiş metinden akış şifresini buradan da anahtarı elde etmek mümkün olabilir. Anahtarların önce başlangıç bitleri ve daha sonra ardışık şekilde diğer kısımları çözülebilmektedir [42].

WEP anahtar ile kimlik doğrulama tek yönlü bir kimlik doğrulama yöntemidir. İstemci erişim noktası tarafından doğrulanmakta, fakat erişim noktası istemci tarafından doğrulanmamaktadır. Ağınıza zarar vermek isteyen bir saldırgan yakınlara bir yere erişim noktası ekleyip normal ağın işleyişini etkileyebilir. Ağa zarar verebilir. İstemciler, farkında olmadan bu erişim noktasına üye olabilir. İstemci güvenilir erişim noktasına bağlandığından asla emin olamaz. WEP anahtar istemci kartı üzerinde ise ve kart çalınırsa, bu kart ağa erişim için kullanılabilir. WEP anahtarların tüm cihazlarda değiştirilmesi gerekir. WEP anahtarları uzaktan değiştirmek mümkün değildir. Tüm cihazlarda bu değişimleri yapmak gerekir, bu uzun bir iştir [43].

IEEE 802.11 tarafından yeni uyarlamalar geliştirilmiştir. IV, 24 bitten 128 bite çıkarılmış, Kerberos V [44] desteği sağlanmıştır. Ortak anahtar uzunluğuda 40 bitten 104 bite uzatılmıştır. Fakat bu yenilikler WEP'in mevcut açıklarını gidememiştir. Cisco ve Microsoft, ortak anahtar yerine dinamik anahtarlar kullanmışlardır. Dinamik anahtarlar, erişim noktalarına dağıtılarak, ağı dinleme yöntemi ile trafik analizi yapılmasını engellemiştir [42].

3.3.2.4. Wi-Fi Korumalı Erişim (WPA - Wi-fi Protected Access)

WPA, Wi-Fi Alliance tarafından geliştirilen bir kablosuz güvenlik teknolojisidir. IEEE, 802.11'deki sorunları çözmek üzere yeni IEEE 802.11i standardı onaylanırken, kablosuz ürün satıcıları Wi-Fi Korumalı Erişim (WPA) olarak bilinen, çeşitli sistemlerin birlikte çalışmasına olanak veren geçici bir standart üzerinde anlaşmıştır.

Wi-Fi Korumalı Erişim, WEP'de varolan şifreleme zayıflıklarını güçlendirir ve şifreleme anahtarlarını otomatik olarak üretmek ve dağıtmak için bir yöntem sunar. Bu çözüm ayrıca, iletişimde alınıp verilen bilgi paketlerinin saldırganlar tarafından değiştirilememesi için veriler üzerinde bütünlük denetimi de sunar. Kuruluş düzeyinde kullanıcı kimlik doğrulamasını geliştirmek için, Wi-Fi Korumalı Erişim ağdaki her kullanıcının kimliğini doğrular ve bu kullanıcıların aldatıcı ağlara katılmalarını engeller. WPA varolan teknolojileri temel alıp, 802.11i ile ileri doğru uyumluluk ve varolan 802.11 çözümleriyle geriye doğru uyumluluk sunarak, WEP ile ilgili zayıflıklara pratik bir çözüm sağlar [45, 46]. WPA, IEEE 802.11i taslak standardının bir altkümesidir. 802.1x Genişletilebilir Kimlik Doğrulama Protokolü (EAP-Extensible Authentication

Protocol) ile Değişken Anahtar Dağıtım (Dynamic Key Distribution) şekillerini Michael (MIC) doğrultusunda birleştirmiştir [47].

WPA kimlik doğrulama

WPA'da 802.1x doğrulaması gerekmektedir. Bu doğrulama 802.11 standardında isteğe bağlıydı. Uzaktan Aramalı Kullanıcı Kimlik Doğrulama Servisi (RADIUS-Remote Authentication Dial-In User Service) altyapısının bulunmadığı durumlarda WPA önceden paylaşımlı şifre yöntemini desteklemektedir. RADIUS altyapısının bulunduğu durumlarda ise EAP ve RADIUS desteklenmektedir [47].

WPA anahtarı yönetimi

WEP den önemli bir fark olarak anahtar yönetimi gösterilebilir. WPA, 2 çeşit anahtarlama kullanılır;

1. Oturum Anahtar kümesi: Bir kullanıcı ve erişim noktası tek nokta(Unicast) arası haberleşmelerde kullanılır.
2. Grup Anahtar kümesi: Ağ içinde herkesin bildiği ve yayın yapılması için kullanılan anahtarlar (multicast, broadcast).

Oturum ana anahtarı ve grup ana anahtarı, ana anahtardan elde edilir. Ana anahtar da doğrulama sırasında doğrulama sunucusu tarafından üretilmiştir. Doğrulama sunucusu olmayan yapılarda bu işlemler erişim noktası tarafından yapılır. Oturum ana anahtarı elde edilen anahtarlar geçicidir. Her yeni cihazla bağlantı yeniden kurulduğunda ya da ağdan çıkılıp girildiğinde yeniden oluşturulur. Grup ana anahtarları da grup geçici anahtarı ile erişim noktaları tarafından belirlenip kullanıcılara dağıtılmaktadır [39].

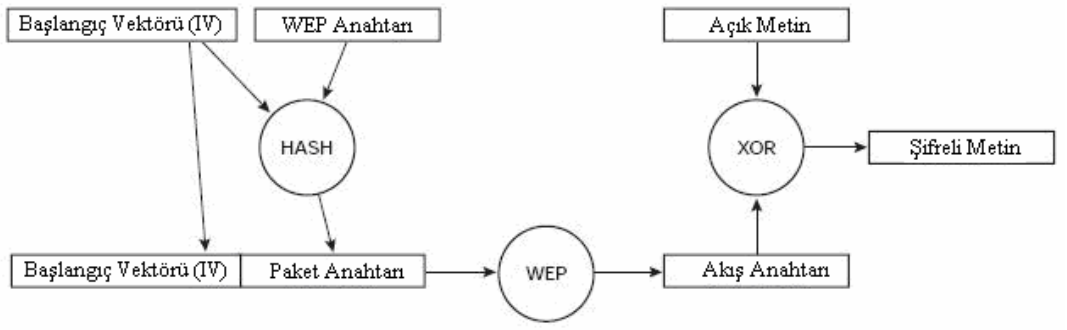
WPA ile tek noktaya ve genel şifreleme anahtarlarının yeniden oluşturulması gerekir. Tek noktaya şifreleme anahtarı için, Geçici Anahtar Bütünlüğü Protokolü (TKIP-Temporal Key Integrity Protocol) anahtarı her çerçeve için değiştirir ve bu değişiklik kablosuz istemci ile kablosuz erişim noktası arasında eşitlenir. Genel şifreleme anahtarı için, WPA, erişim noktasının değiştirilmiş anahtarı bağlantılı kablosuz istemciye duyurmasını sağlayan bir araç içerir [45].

Geçici Anahtar Bütünlüğü Protokolü (TKIP)

Geçici Anahtar Bütünlüğü Protokolü, IEEE 802.11i standardıdır. Mevcut ürünlerin donanımında değişiklik yapmadan, sadece yazılımsal değişiklik yaparak güvenli veri transferi sağlamak maksadıyla geliştirilmiştir. TKIP, RC4 akış şifreleyici algoritma üzerine kuruludur.

TKIP'de başlangıç vektörü 48 bit'e çıkarılmıştır. IV, hem paketlere sıra numarası vermek hem de her paket için tek kullanımlık anahtar üretiminde kullanılır. Paketlere sıra numarası vermek tekrar (replay) saldırılarını önlemek içindir. Ayrıca sırasız gelen paketler alıcı tarafından atılmaktadır. 48 bit IV ve aynı geçici anahtar (TK-Temporal Key) ile üretilecek tek kullanımlık anahtarlar yaklaşık 100 yıl sonra tekrarlanmaktadır.

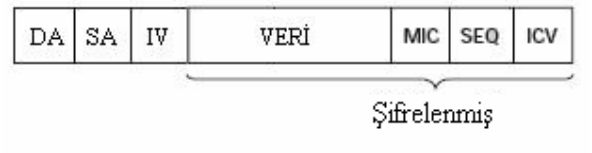
Her paket için kullanılan IV değeri TKIP'de değişmektedir. Bu yöntemde zayıf anahtar üretiminden faydalanan saldırıları önlemektedir [27, 42, 48].



Şekil 3.12: TKIP paket anahtarı oluşturma

Mesaj Bütünlük Kodu (MIC-Message Integrity Code)

WEP'teki ICV'nin zayıflıklarına, WPA ile Michael olarak bilinen bir yöntem, 8 baytlık bir ileti bütünlüğü kodu (MIC) hesaplayan yeni bir algoritma tanımlamaktadır. MIC alanı, çerçeve verileri ve ICV ile birlikte şifrelenir. Alıcı ve gönderen MAC adresleri ve mesaj bir anahtarlama işlevi (hashing) fonksiyonuna tabi tutulur ve 8 baytlık bir çıktı oluşur. MIC, IEEE 802.11 çerçevesinin veri bölümü ile 4 baytlık ICV arasına yerleştirilir, çerçeve verileri ve ICV ile birlikte şifrelenir. MIC, kaynak ve varış MAC adreslerini ve veriyi alarak sağlama bitleri (cheksum-squence number) oluşturur. Bu sağlama bitleri verinin sonuna şifrelenerek eklenir. Bu yöntem mesaj içeriğinin değiştirilmesini önler. MIC lineer algoritma kullanmaz. ICV gibi zayıflıkları yoktur [27, 39, 42].



Şekil 3.13: MIC çerçeve yapısı

3.3.2.5. Çok Güvenli Ağ (RSN-Robust Security Network, WPA2)

IEEE 802.11i standartlarına uygun yeni bir protokol geliştirilmiştir. Bu protokol WEP üzerine kurulmamış yeni ve farklı bir yapı olarak geliştirtmiştir. RSN, WEP'i desteklemez, WPA ile uyumlu olarak çalışmaktadır.

RSN, doğrulamayı ve anahtar yönetimini IEEE 802.1x standartları ile gerçekleştirir. Veri bütünlüğü MIC ile sağlanır, gezginlik (roaming) sağlar. Gezginlik gerçek zamanlı iletişimlerde veri kaybını engeller. RSN gezginliği iki farklı şekilde gerçekler;

- Önceden Doğrulama: Kullanıcı bir erişim noktasına bağlı iken diğer bir erişim noktasının varlığının farkına varırsa 802.1x anahtar değişimi ile bu erişim noktası için de anahtarları elde eder ve saklar. Sinyal zayıflığı gibi nedenlerden önceden anahtarını elde ettiği erişim noktasına geçmek isterse 802.1x işlemlerini yapmaz.

- Anahtar önbellekleme: Erişim noktası ile daha önceden anahtar belirlendiyse bu anahtarlar bellekte saklanır. Bu erişim noktası ile iletişime geçildiğinde 802.1x işlemlerini tekrarlamaz.

RSN'de şifreleme TKIP veya Sayaç Modu ile Zincirleme Blok Şifreleme Mesaj Doğrulama Kodu (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol-CCMP) ile gerçeklenir. CCMP zorunlu iken, TKIP ise seçeneklidir [39].

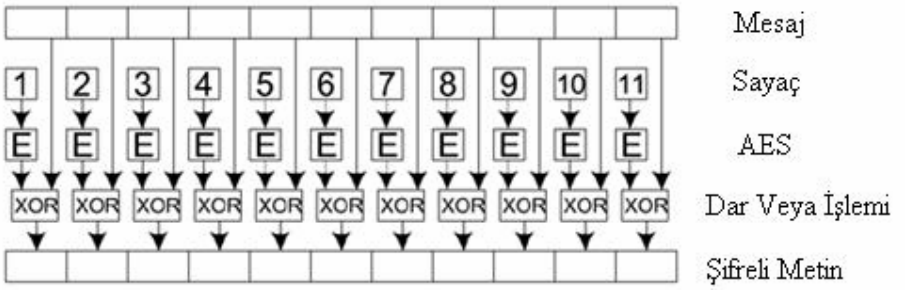
Sayaç Modu ile Zincirleme Blok Şifreleme Mesaj Doğrulama Kodu (CCMP)

CCMP, IEEE 802.11i protokolünün yeni şifre yöntemidir. Gelişmiş Şifreleme Standardı (AES-Advanced Encryption Standard) kullanır. AES birçok farklı kipte kullanılabilir. IEEE 802.11i standardı, Sayaç Modu ile Zincirleme Blok Şifreleme Mesaj Doğrulama

Kodu kullanır. Anahtar uzunluğu 128 bittir. CCMP'de başlangıç vektörü kullanır ve 48 bit uzunluğundadır. Paketlere sıra numarası verir, daha sonra diğer bilgilerle beraber mesaj bütünlük kodu oluşturmak ve paket şifrelemek için AES şifreleme algoritmasında parametre olarak kullanılır [42]. AES, blok şifreleme olan Rijndael algoritması ile 128, 192 ve 256 bitlik anahtarlar kullanır. 802.11i standardında AES kullanmak zorunludur [27].

Sayaç Modu (Counter Mode)

Sayaç yönteminin kullanılma amacı aynı veri içeren bloklar aynı şifre ile şifrelendiğinde farklı çıkışların olmasının istenmesidir. Çünkü mesajın tekrar eden bloklardan oluştuğunun bilinmesi bir zayıflıktır. Gizliği sağlamaktadır. Veri blokları şifrelenmiş sayılar ile dar veya işlemine tutulmaktadır. Burada kullanılan sayılar rasgele seçilmektedir çünkü aynı iki mesaj aynı çıkışları verecektir. Bu sayının başlangıcı karşı tarafa iletilmelidir. Bu modda 128 bitlik şifreleme anahtarı kullanılır [39, 48].



Şekil 3.14: AES sayaç çalışma modu

Zincirleme Blok Şifreleme Mesaj Doğrulama Kodu (CBC- MAC)

Zincirleme Blok Şifreleme Mesaj Doğrulama Kodu (CBC-MAC-Chaining Message Authentication Code) modu ise MIC hesabında kullanılır. Eğer mesajda 1 bit değişirse MIC de büyük değişiklikler olur ve tahmin edilemez. MIC hesabı geri dönülmez bir şekilde yapıldığı için araya girenin mesaja uygun bir MIC hesaplaması mümkün değildir.

İlk veri bloğunu alır ve AES i kullanarak şifreler, sonuç ile 2. bloğu dar veya işlemine tutar ve şifreler, çıkan sonucu bir sonraki blok ile dar veya işlemine tutar ve şifreler.

CCMP çalışma yapısında öncelikle MIC hesabı için CBC-MAC kullanılır. Buradan oluşan 128 bitin 64 biti kullanılır.

Mesajın şifrelenmesinde de sayaçtan bir değer alınır ve AES algoritması ile şifrelenip daha sonra çıkan sonuç mesajın 128'lik ilk bloğu ile dar veya işleminden geçer. Daha sonraki bloklarda sayaç birer arttırılarak elde edilen sayılar kullanılarak şifrelenir [39].

3.3.2.6. Genişletilebilir Doğrulama Protokolü (EAP-Extensible Authentication Protocol)

EAP ağ yöneticisine kendi kurumunun güvenliği için en iyi çözümü seçmekte esnek olma ve bunu ihtiyaçlarına göre gelecekte değiştirebilme izni verir. EAP'ler tasarımlarında kurulmuş olan bazı farklı yöntemlere göre sınıflanabilirler.

Kurumsal modda doğrulama, ayrıca noktadan-noktaya ağlar için de uygulanabilecek IEEE 802.1x standardı ile yönetilmektedir. 802.1x doğrulama isteyen birinin doğrulanmasının doğrulama sunucusu tarafından yapılmasını önermektedir. WLAN'ın içyapısal modunda istemci kablosuz bir kullanıcı ya da cihazdır, yetkilendirici istemcinin iletişime geçmek istediği erişim noktasıdır ve doğrulama sunucuyu bir doğrulama, yetkilendirme ve hesap yönetimi (authentication, authorization, accounting AAA,) sunucusudur ya da RADIUS hizmetidir [37].

802.1x, kablolu Ethernet ağlarına ve kablosuz 802.11 ağlarına kimliği doğrulanmış ağ erişimi sağlamak için kullanılan bir IEEE standardıdır. IEEE 802.1x, merkezi kullanıcı tanımlama, kimlik doğrulama, dinamik anahtar yönetimi ve hesap oluşturma desteği sağlar. 802.1x standardı, bilgisayarın ve ağın birbirlerinin kimliğini doğrulamalarına izin vererek, kablosuz bağlantılar üzerinden veri şifreleme için kullanıcı veya oturum bazında anahtarlar oluşturarak ve anahtarları dinamik olarak değiştirmeye olanak vererek güvenliği geliştirir [46].

Mevcut standartlar kurumsal düzeyde güvenlik için tam bir spesifikasyon içermemektedir. Sisteme olası saldırıları ve yetkilendirilmemiş girişleri engellemek için anahtar düzenli olarak değiştirilmeli ve ağdaki kullanıcılar ve cihazlara bununla ilgili

olarak bilgi verilmelidir; ancak 802.11 protokolünde de bu değişiklik merkezi bir biçimde yapılamamaktadır.

Ancak, ağ ve kullanıcı ya da cihaz birbirlerini karşılıklı olarak doğrulayacaklardır. 802.1x doğrulama işleminin yöntemini belirlemez. Bir ağın güvenlik ihtiyaçları için farklı seçeneklerin seçilebilmesine olanak verir [37].

802.1x–2001 standardı şudur;

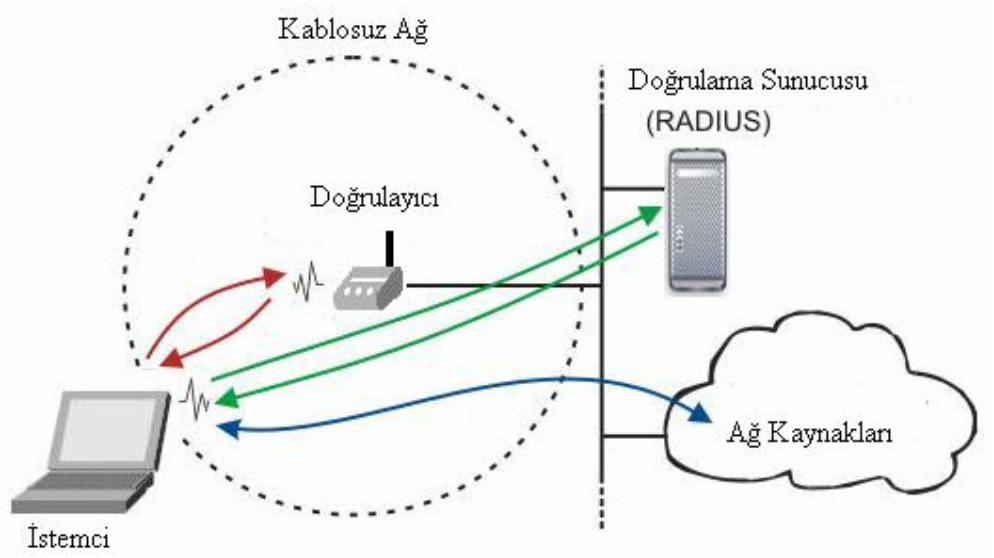
Port tabanlı ağ erişim denetimi, noktadan-noktaya bağlantı özelliklerine sahip bir yerel ağ portuna takılan cihazların kimlik doğrulaması ve yetkilendirme için ve bu sayede kimlik doğrulaması ve yetkilendirmesi başarısız olması durumunda o portu erişimden koruyarak yerel ağ altyapılarının fiziksel erişim özelliklerinin kullanımına olanak sağlar. Bu bağlamda bir port, yerel ağ altyapısına ekli tekil bir noktadır [49].

EAP doğrulaması için aynı şemaya bağlı kalarak ve RC4'ün veri şifreleme modlarının seçilmesine izin vererek veri şifrelemeyi kuvvetlendirerek ya da WEP ve WPA gibi daha önceki protokollerde kullanılan RC4 algoritmasına göre saldırılara karşı daha güvenli olan gelişmiş bir CCM blok şifresi modunda gelişmiş şifreleme sistemi (AES) ile güvenliği güçlendirir [37].

802.1x ile Kimlik Doğrulama

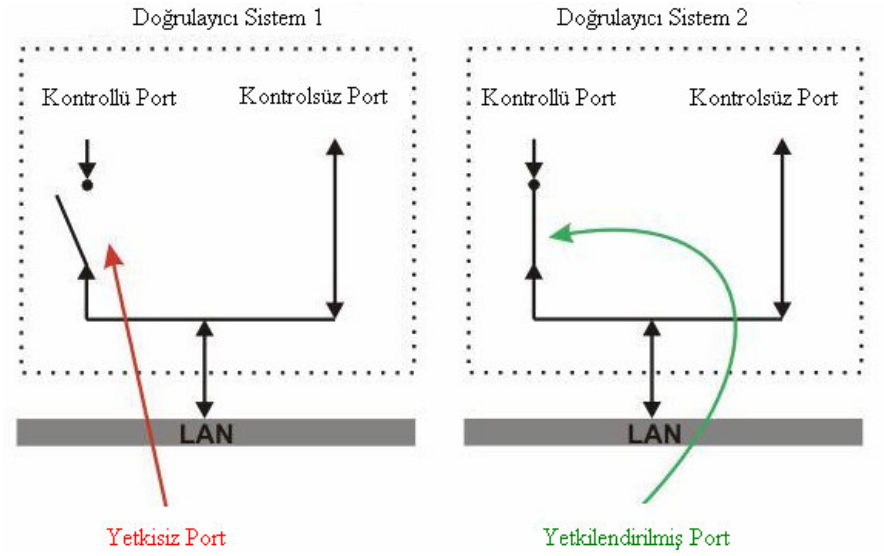
1) İstemci, doğrulayıcıya bağlantı talebinde bulur.
2) Doğrulayıcı bağlantı isteğini alınca, tüm portları kapalı tutar, sadece istemci ile arasında bir port açar.
3) Doğrulayıcı, kullanıcıdan kimliğini ister. İstemci kimliğini gönderir, doğrulayıcı kimlik bilgisini doğrulama sunucusuna gönderir. Kimlik gönderildikten sonra kimlik kanıtlama süreci başlar. İstemci ve doğrulayıcı arasında kullanılan protokol EAP kaplamalı yerel ağdır (EAPOL). Sunucu kimliği doğrular ve doğrulayıcıya gönderir. Doğrulayıcı, istemcinin portunu yetkilendirilmiş duruma getirir.

4) İstemci, doğrulama sunucusundan, onun kimliğini ister. Doğrulama sunucusu, kimlik bilgisini istemciye gönderir.
5) İstemci, doğrulama sunucusunun kimliğini doğruladığında, veri trafiğine başlanır [42, 49].



Şekil 3.15: 802.1x ile kimlik doğrulama

Kimlik kanıtlama öncesinde sadece denetimsiz port açıktır. Sadece EAPOL trafiğine izin verilir. İstemci kimliği kanıtlandıktan sonra, denetimli port açılır ve diğer yerel ağ kaynaklarına erişim hakkı verilir [49].



Şekil 3.16: Denetimli portun kontrol durumu

802.1x Anahtar Yönetimi

1) İstemci ve doğrulama sunucusu doğrulama yaparken sunucudan gönderilen doğrulamanın başarılı olduğunu söyleyen son iletilerden biri bir Ana Anahtar'dır (MK-Master Key). Gönderildikten sonra MK sadece istemci ve doğrulama sunucusu tarafından bilinir. MK, istemci ve doğrulama sunucusu arasındaki bu oturuma bağlıdır.

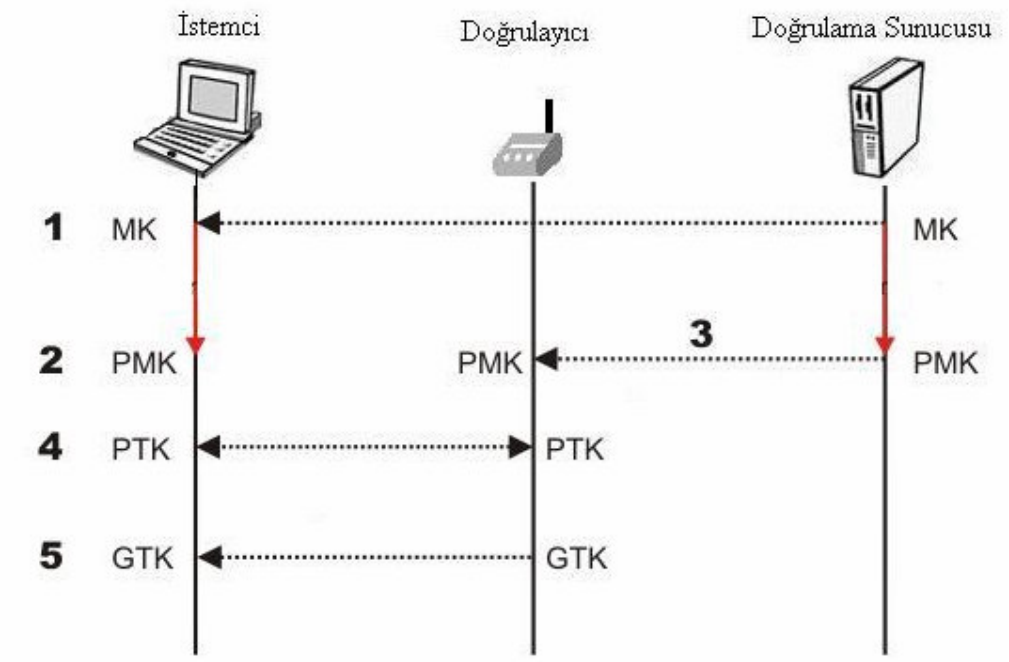
2) Hem istemci hem doğrulama sunucusu, MK'dan bir Çiftli Ana Anahtar (PMK - Pairwise Master Key) üretir.

3) O zaman PMK doğrulama sunucusundan doğrulayıcıya taşınır. PMK'yi sadece istemci ve doğrulama sunucusu türetebilir, bunun yanında doğrulayıcı, doğrulama sunucusunun yerine erişim-denetim kararları verebilir. PMK, istemci ve doğrulayıcı arasındaki bu oturuma bağlı yepyeni bir simetrik anahtardır.

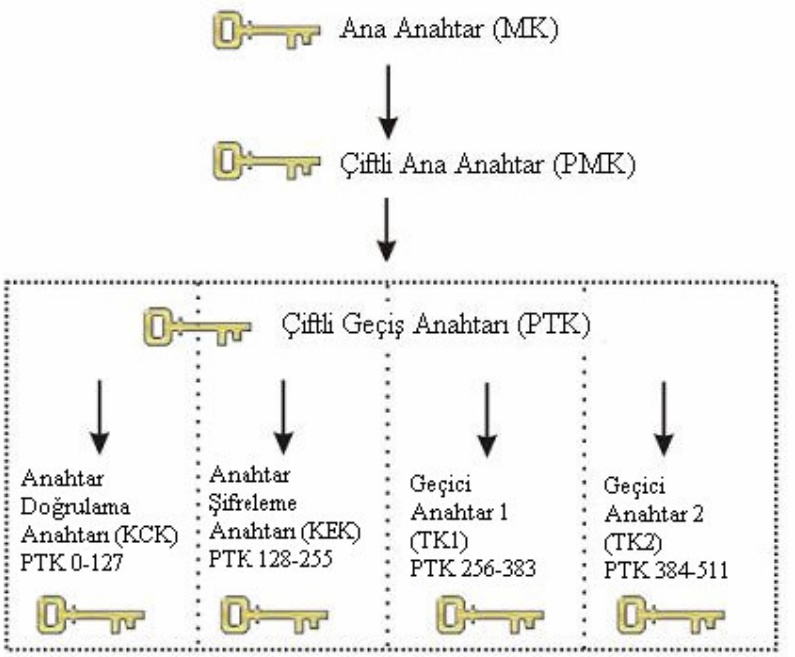
4) Çiftli Ana Anahtarı türetmek, bağlamak ve doğrulamak için istemci ve doğrulayıcı arasında PMK ve 4 yönlü el sıkışma (handshake) kullanılır. Çiftli geçiş anahtarı (PTK-Pairwise Transient Key) işletimsel anahtarlar topluluğudur:

- Anahtar Doğrulama Anahtarı (KCK-Key Confirmation Key), PMK'ye sahipliği kanıtlamak ve PMK'yi doğrulayıcıya bağlamak için kullanılır.
- Anahtar Şifreleme Anahtarı (KEK-Key Encryption Key), Grup Geçiş Anahtarı (GTK-Group Transient Key) dağıtımı için kullanılır.
- Geçici Anahtar 1 ve 2 (TK1/TK2 - Temporal Key 1 and 2) şifreleme için kullanılır. TK1 ve TK2'nin kullanımı şifreleme türüne özeldir.

5) KEK ve 4 yönlü grup el sıkışması doğrulama sunucusundan istemciye GTK göndermek için kullanılır. GTK, aynı doğrulayıcıya bağlı tüm istemciler arasında paylaşılan bir anahtardır ve çoğa gönderimli iletişim akışını güvenli kılmak için kullanılır [49].



Şekil 3.17: 802.11i'de 802.1x ile anahtar yönetimi



Şekil 3.18: Ana oturum anahtarı

Güvenli WLAN'lar oluşturmak için EAP'de zorunlu, önerilen ve opsiyonel gereklilikler bulunmaktadır;

Zorunlu Gereklilikler

Simetrik bir anahtarlama materyalinin üretilmesi: Doğrulama-sonrası anahtar kaynağında ve ayrıca da veri aktarımlarını şifrelemede kullanılmak üzere özgün anahtarları üretme yeteneği.

Karşılıklı doğrulama desteği: Bu özellikte cihaz erişim noktasına doğrulanabilir ve erişim noktası ve ağda cihaza doğrulanabilir. Aralarında karşılıklı doğrulama bulunmaktadır.

Kendini-Koruma: Bu, aktarımda kullanılan mesajları kurcalayan herhangi bir tarafın kullanıcılar hakkında bilgi edinmesine mani olmak için. Yöntemin korsanlık ve gizlice edinmeye karşı kendini koruması.

Durum eşleme: Yöntemde tesis edilmiş olan ve protokol, anahtarlar ve kullanılan veri şifreleme modu gibi belli durum özelliklerinin bu aktarımdaki taraflarca

değiştirilebileceği mekanizma ve aktarım değişimi tamamlandığında durum eşitlenmelidir.

Sözlük saldırılarına karşı direnç: Yetkilendirilmemiş kullanıcıların bir şifre listesi kullanarak ağa girmesine mani olmak gibi sistemin saldırılara karşı savunmasızlığına mani olmak için ağın güvenliğini garanti altına alan bir mekanizma olmalıdır.

Ortadaki adam saldırısı durumuna karşı koruma: Yöntem herhangi bir yetkilendirilmemiş kullanıcının saldırılarına karşı ya da bir kullanıcıyı ağ içinde bağlanmak istediği erişim noktası dışında başka doğrulanmış olarak başka bir erişim noktasına bağlanmaya ikna etmeye çalışan bir saldırgana karşı açık olmamalıdır.

- Şifreli bağlama kullanıcı ve sunucunun doğrulama süresi boyunca tek bir bütün olarak hareket etmesini garanti eder.
- Bütünleme koruması doğrulamada yer alan her iki tarafın da değiştirdikleri mesajları el değmemiş olarak almalarını garanti eder.
- Tekrarlama koruması kullanıcı ile doğrulayan arasındaki diyaloglarının bir saldırgan tarafından ağa girmek için tekrarlanmasına karşı koruma sağlar.
- Oturum bağımsızlığı tek bir oturumdaki saldırının daha önceki yada takip eden oturumlardaki saldırılarla bağdaşmamasını garanti eder.

Korumalı şifre takımı görüşmesi: Doğrulamayı korumak için kullanılan görüşülen şifre tipi korunmalıdır.

Önerilen Gereklilikler

Parçalanma: Sınırlı büyüklükte aktarımların üstünde işlemler gerçekleştiriliyor olabilir, buna göre yöntemin işlemleri ufak kısımlara bölebilme ve daha sonrada bunları birleştirme yeteneği olmalıdır.

Son-Kullanıcı kimliğinin gizlenmesi: Mesaj değiştirenlerin kimliği bu kimselerin kimliğini açıklamamak için şifrelenmelidir.

Opsiyonel Gereklilikler

Kanal bağlaması: Bu özellikte doğrulayıcının son nokta belirleyenleri düşük katmanlı protokollerce aktarılabilir.

Hızlı yeniden bağlanma: Güvenlik bağlantısı kesilmişse ve yeniden kurulması gerekiyorsa yeniden bağlanmanın daha az sayıda mesajla yapılması gerekmektedir.

Kurumsal Gereksinimler

Kablosuz ağlarda güvenlik, kurumların tek ilgi alanı değildir, fiyat, kullanıcı uygunluğu ve mevcut kablolu sisteme uyum gibi özellikler kurumların ihtiyaçlarını dengelemelidir. Hiçbir güvenliği olmayan ya da yetersiz güvenliğe sahip olan çeşitli kablosuz ağlar bulunmaktadır. Mevcut yazılımları kullanan EAP yöntemi bunlar için avantajlı olacaktır. Kablolu ağlar daha önce herhangi bir kablosuz erişim noktalarına sahip olmayan kablosuz ağlara göre daha yaygındır ve sistem mimarisinde en az değişimi gerektiren EAP yöntemi tercih edilebilir.

EAP Yöntemleri

Yukarıda bahsedildiği gibi 802.1x standardı EAP'yi noktadan-noktaya ağlarda kullanmayı buyurur ve doğrulama için bir yöntem, algoritma ya da yordam belirlemez ancak belli bir metodun iliştirilebileceği bir çerçeve belirler. EAP yöntemleri kablosuz ağlar ve buna ek olarak kablolu ağlar için geliştirilmişlerdir. Bu doğrulama için sertifika yerine şifre kullanan yöntemlerin yanı sıra açık anahtar şifrelemesi ve sertifika kullanımına dayalı olarak kurulmuş yöntemleri içerir.

Mesaj Özü ile EAP (EAP-MD5- Message Digest Five)

Bu yöntemde mekanizma doğrulanacak kullanıcıdan kullanıcı adı ve şifre alarak ve bunu MD5 mesaj hashing algoritması ile şifreleyerek ve bu veriyi de RADIUS sunucusuna naklederek çalışır. Bu basit bir yöntemdir ve uygulaması kolaydır ancak önemli eksikleri bulunmaktadır ve zaman içinde anahtarlar sabit kaldığı ve değişmediği için güvenli bir EAP yöntemi olarak değerlendirilemez. Buna ek olarak MD5 şifrelemesi, kablosuz ağlar üzerinden EAP'ya gönderme yapılarak belirlendiği gibi her

iki yönde de istemci ve erişim noktası arasında simetrik bir doğrulama gerekliliğini yerine getiremez. Bu ise bu yöntemi ortadaki adam saldırılarına karşı açık hale getirir.

Taşıma Katmanı Güvenliği ile EAP (EAP-TLS-Transport Layer Security)

Bu yöntem EAP çerçevesi içinde açık anahtar sertifika doğrulama yordamı kullanarak kurulmuştur ve müşteri ve doğrulayıcı sunucu arasında her iki yönde de karşılıklı doğrulama getirir. Bu karşılık olarak kabul edilmiş bir yetkili tarafından kabul edilmiş bir açık anahtar sertifikasına sahip istemci ve erişim noktası için zorunludur. Bu yöntemde yüksek oranda güvenlik vardır ancak açık anahtar altyapısına ihtiyaç duymaktadır ve bu da kuruma yeni giderler getirecektir.

Tünellenmiş Taşıma Katmanı Güvenliği ile EAP (EAP-TTLS-Tunneled Transport Layer Security)

Bu yöntem TLS'nin tünellenmiş TLS bir uzantısıdır. Bir açık anahtar algoritması ve karşılıklı olarak kabul edilmiş bir yetkili tarafından verilen bir sertifika kullanan istemci ile sunucu arasında güvenli bir tünel kurularak işler.

Korunmuş EAP (PEAP-Protected EAP)

Korunmuş EAP (PEAP) TTLS'ye benzer bir şekilde davranan bir EAP yöntemidir. Şifrelendirilmiş edilmiş bir tarzda yetkilendirilmiş bir işlemi yapmak üzere bir TLS yaratır. Şifrelendirilmiş tünel içerisinde potansiyel olarak daha az güvenli başkaca bir yetkilendirme yöntemi kullanılabilir. Ancak, TTLS'nin tersine, PEAP diğer yönde değil de, yetkilendiriciyi istemci için yetkilendirir. Bu da sertifikaların istemcilerde değil de, sadece yetkilendiricilerde mevcut olmasını gerektirerek karmaşıklığı ve maliyeti azaltır. PEAP'ın faydaları arasında mesaj yetkilendirilmesi ve şifrelendirme, karşılıklı olarak güvenli anahtar değiştirilmesi, parçalara ayırma ve yeniden birleştirme gücü ve hızlı yeniden bağlanma sayılabilir. PEAP en güvenli yöntemlerden biridir, fakat hem Microsoft hem de Cisco farklı uygulama yöntemlerini desteklediğinden evrensel olarak kabul görmemiştir.

Şifreye Dayalı Yöntemler

Şifreye dayalı yetkilendirme yönteminin kullanılmasının sertifikaya dayalı bir yöntemin kullanılmasına göre bazı avantajları vardır. Bu avantajlardan en önemlileri ise maliyet avantajı ve kullanım kolaylığıdır. Sertifika satın alınması gerekmediğinden ya da kuruluş için kendi-sertifika yetki kurulumu gerekli olduğundan maliyet daha azdır. Kullanıcıların şifreli anahtardan ziyade kolay hatırlanabilir bir şifre kullanmalarını müsaade ettiği için kullanım kolaylığı gelişir. Ancak, sertifikaya dayalı yöntemlerin tersine, şifreye dayalı yöntemler sözlük saldırılarına mazur kalabilir.

LEAP (Sadeleştirilmiş Genişletilebilir Yetkilendirme Protokolü- Lightweight Extensible Authentication Protocol)

Sadeleştirilmiş Genişletilebilir Yetkilendirme Protokolü Cisco tarafından geliştirilmiştir ve Cisco'nun sunucu ile istemci arasında karşılıklı yetkilendirmeye dayalı ve kullanıcı adı/şifre çizelgesi kullanan EAP için geliştirdiği ve mülkiyet hakkı Cisco'ya ait olan bir yöntemdir. LEAP her oturum için anahtarlar yaratarak oturum bağımsızlığını geliştirir, böylelikle de tek bir oturuma bir saldırı yapılsa bile daha önceki ve sonraki oturumları güvenli kılar. Ayrıca, cihaza trafiğin iletilmesine müsaade etmeden önce bütün bağlantıları yetkilendirerek hizmetin reddedilmesine ya da hizmetin çalınmasına karşı yapılan saldırılara karşı da korunmada yardımcı olur. Ancak, LEAP şifreye dayalı bir yöntem olduğundan ve meydan okuma ve tepki verme diyalogu şifrelenmiş tünel vasıtasıyla olmadığından, sözlük saldırılarına maruz kalır. Yine de, güçlü bir şifre politikasıyla birlikte uygulanırsa, LEAP, ek bir karmaşıklığa ya da açık sertifika anahtarlarının kullanılması nedeniyle oluşacak maliyetlere neden olmadan WEP'e göre kayda değer oranda güvenlik avantajı sağlayabilir.

Basit Şifre Üstel Anahtar Değişimi (SPEKE-Simple Password Exponential Key Exchange)

SPEKE, ya da, Interlink Networks'un sahip olduğu bir EAP yöntemidir. SPEKE yöntemi görünürdeki rast gele içeriklerin değiş tokuş edilmesi için bir dizi mesajın yaratılmasında hem yetkilendiricide hem de müşterideki karşılıklı olarak sahip olunan şifre bilgisini kullanır. Şifrenin doğruluğuna her iki taraf da mutabık kaldıktan sonra ilerdeki kullanımlar için cihazlar arasında ana oturum anahtarı paylaşılacaktır. Bu yöntemin fazladan sahip olduğu kuvvetli yön, rastgele olarak büyük bir modül

numarası için büyük bir asal sayı yaratan bir açık anahtar yaratmasından kaynaklanır ki bu da onu tersine çevirmek için gerekli olan ayrık logaritmik işlevlerin yerine getirilmesini göreceli olarak zorlaştırmasından dolayı etkin bir şekilde tek yönlü bir fonksiyon sağlar.

SPEKE yönteminin avantajı sertifika uygulamadan anahtar transferi ve yetkilendirme yordamları için açık anahtar şifrelendirme yöntemlerinin güvenliğini kazanır. Buna ek olarak, mekanizma diğer şifreye dayalı yöntemlere nazaran sözlük saldırılarına karşı daha az duyarlıdır.

Üye Kimlik Modülü ile EAP (EAP-SIM Subscriber Identity Module)

Bugün hücresel donanım sağlayıcıları tarafından kullanılan mevcut standart yetkilendirme yöntemini sağlayan Üye Kimlik Modülleri kullanarak EAP için yeni bir yöntem sunmak üzere taslak çalışmalar devam etmektedir. EAP yöntemi çeşitli veriler için bir depo sağlayabilecek akıllı kart-benzeri bir cihazı kimlik kanıtları olarak kullanır. İstemciler doğrulama yordamlarında SIM'ler üzerinde bulunan kimlik kanıtları sağlamak üzere bu SIM'leri kullanır.

Kimlik gizliliği sanal adlar mekanizması yoluyla sağlanır ve ana anahtardan anahtar türetilmesini sağlar. Prosedür veri şifrelendirme için bir dizi anahtar yaratmak için bir dizi rastgele isteklerin kullanılmasıyla bir meydan okuma ve tepki yöntemine dayalıdır. Bu yöntemin fiziksel cihazı bir anahtardan ya da şifreden ziyade kimlik kanıtları olarak kullanılmasını mümkün kılan bir avantajı vardır, ancak bir kullanıcı ya da cihaz tarafından bütün oturumlar için bir SIM kartının yeniden kullanımında olduğu gibi oturum-bağımsızlığı yoktur.

Doğrulama ve Anahtar Mutabakatı ile EAP (EAP- AKA Authentication and Key Agreement)

EAP-AKA, EAP-SIM'in hafifçe değiştirilmiş olan bir sürümüdür. Bu standart kullanıcı hizmet kimlik modülleriyle EAP-SIM ve GSM ağlarında kullanılan SIM kartlarının yerini alır. Her ne kadar EAP-SIM ile EAP-AKA arasındaki yordamlar ve yöntemler benzeşse de, EAP-AKA ortak yetkilendirme için kalıcı anahtarların kullanımı nedeniyle daha güçlü bir güvenlik seviyesi sağlar.

Sertifikaya Dayalı Yöntemlerle İlgili Konular

Sertifikaya dayalı EAP tiplerinin çoğu avantajlarına karşın bazı dezavantajları da vardır;

Yönetim Maliyeti: Sertifikalar kavramı kullanımdaki sertifikaların geçerliliğini onaylayacak ve her iki tarafça da güvenilir bir üçüncü tarafın olacağı bir durumu varsayar. Bu gereklilik nedeniyle, ciddi maliyetler söz konusudur. İster sertifikalar bütün cihazlar için dışarıdan iyi-bilinen bir sağlayıcından alınmış olsun, isterse de kuruluşun kendi sertifikalarını yapması ve merkezi yetkili olması için bir yazılım ve gerekli eğitim ve yordamları kendisi oluştursun her iki durumda da ciddi bir maliyet söz konusu olacaktır.

Yüksek Seviyeli Protokol Değişimi: Bir ağ üzerinde yetkilendirmeyi sağlamak için kullanılacak sertifikaya dayalı EAP yöntemleri karşılaştırmalı olarak bakıldığında karşılıklı olarak daha uzun mesaj değişimini gerektirir. Bunun da karşılıklı değişimi tamamlamak için gerekli süreyi uzatmak ve bunun yapılması için gerekli hesaplama gücünü arttırmak gibi bir dezavantajı vardır. Bir dolaşım senaryosunda harcanan zaman dezavantaj yaratacaktır. Yine hesaplama gücü için gereken artış da PDA'lar gibi küçük ve bağımsız cihazlar için kötü olacaktır.

Kullanıcıyı Doğrulayamama: Sertifikaya dayalı yöntemler içerisinde hangi sertifika programlanmışsa o yetkilendirilir; hemen hemen her durumda bu kullanıcıdan ziyade cihazdır. Bu da cihazlar üzerinde bir tasarrufta bulunulduğu zaman ağı tehlikelere maruz bırakır.

Aşağıda Tablo 2,1'de ortaya atılan EAP için hem yöntemlerin hem de teknolojilerin kısa bir gözden geçirilmesi vardır.

İster kablolu isterse de kablosuz olsun bir ağı güvenli yapmak için, EAP prosedürleri içerisinde bile EAP yönteminin uygulanması önemli bir aşamayken yine de açıklanması gereken güvenlik sorunları ve maruz kalmalar vardır.

Tablo 3.1: Kablosuz ağlar için EAP gereklilikleri

Gereklilikler	EAP-MD5	EAP-TLS	EAP-TTLS	EAP-LEAP	EAP-PEAP	EAP-SPEKE
Anahtarlama materyalinin oluşturulması	Hayır	Gerekli değil	Evet	Evet	Evet	Evet
Karşılıklı yetkilendirme	Hayır	Evet	Evet	Evet	Evet	Evet
Kendini koruma	Evet	Evet	Evet	Evet	Evet	Evet
Sözlük saldırısına direnme	Sadece daha uzun şifrelerde	Evet	Evet	Hayır	Evet	Evet
MITM saldırısına karşı korunma	Hayır	Evet	Evet	Evet	Evet	Evet
Korunmuş Uzlaşılı Şifre Demeti	Hayır	Gerekli değil	Evet	Evet	Evet	Evet
Kullanıcı Kimlik saklanması	Hayır	Hayır	Evet	Hayır	Evet	Hayır
Daha hızlı yeniden bağlanma	Hayır	Hayır	Evet	Hayır	Evet	Hayır

Muhtemel Saldırılar

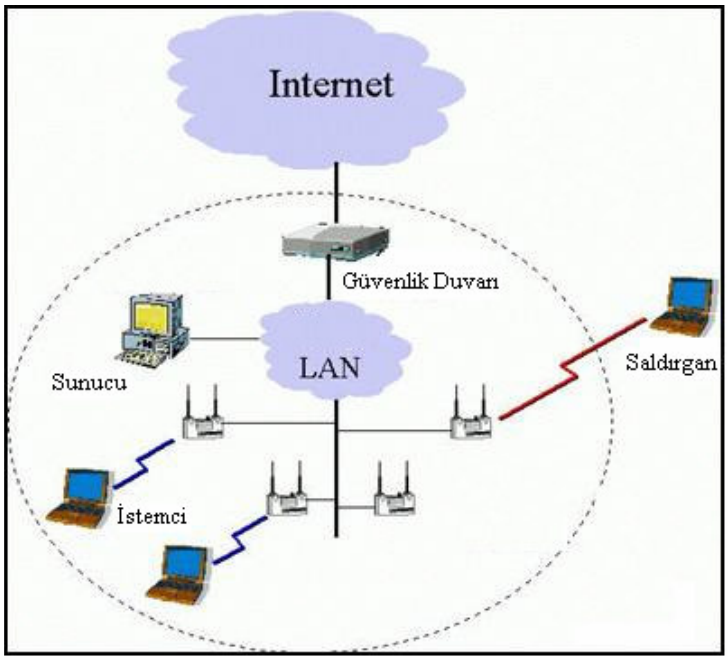
Kullanıcıları ya da cihazları güvenli bir şekilde bir ağa yetkilendirmek için EAP yönteminin kullanılmasının her zaman güvenliği garanti ettiği söylenemez. EAP yordamına karşı saldırılar olabilir. Güvenli bir EAP yönteminin bu tür saldırılara karşı korunması olacaktır. EAP yöntemine karşı yapılması muhtemel saldırıların bazıları şunlardır;

- Şifresiz yetkilendirme değişimlerini okuyarak kullanıcı kimliklerinin keşfedilmesi.
- EAP paketlerini alıp değiştirmek ve aldatmak. Aldatıcı yetkilendirme cevapları, yeniden tekrarlı gönderme saldırıları, ya da örtüşen kimlik tanımlayıcılarıyla paketler kullanarak hizmetin engellenmesi
- Sözlük saldırısı, yetkilendirme değişimini devre dışı bırakmaya tahrik ederek erişim sağlamak için ortak şifreleme listesi kullanmak.
- Eğer EAP yöntemi güvenli olmayan anahtar oluşturma teknikleri kullanıyorsa anahtarların toparlanması.

- Saldırganın bağlanmak isteyen müşteri için güvenlikli ağa kendisini bir erişim noktası olarak gösterdiği ama aslında böyle bir ağ olmadığı durumda ortadaki adam saldırıları
- Daha sonraları bir karşı saldırının yapılması için daha kolay olan daha az güvenli bir tipine müdahale etmek için kullanılan şifreleme de dahil olmak üzere şifreleme parametrelerinin tipine müdahale etmek
- Yetkilendiriciyi tahrik etmek veya istemci ya da EAP yetkilendirici sunucuya yanlış bilgi vermek [37].

3.4. SALDIRI TÜRLERİ VE ARAÇLARI

Kablosuz ağlara saldırılar amaçlarına göre sınıflandırılmıştır. Yapılan saldırı şekline göre kullanılan yöntemler ve araçlar farklılık gösterir.



Şekil 3.19: Saldırganın ağdaki konumu

3.4.1. Saldırı Türleri

Kablosuz ağlara saldırı yöntemleri 3 kategoride toplanmıştır;

- Keşif saldırıları
- Giriş saldırıları
- Hizmeti engelleme saldırıları (DoS-Denial of Service)

Tüm belirgin saldırı araçları, scriptler, kodlar bu kategorilerin biri içinde yer alır. Kablosuz çevrelerde saldırı girişimlerinde keşif uygulamaları ve giriş araçları birleştirilerek uygulanır. İnternet solucanları gibi, bazı ataklar script veya programların bir birleşimi olabilir. WLAN aygıtları solucanlardan ve virüslerden etkilenmez. Fakat bu tür saldırılar ağdaki bilgisayarlara kötü niyetli programların daha hızlı yayılmasına neden olabilir [27].

3.4.1.1. Keşif Saldırıları

Keşif saldırıları, izinsiz şekilde sistem haritasını, hizmetlerini veya açıklarını keşfetmeye çalışır. Aynı zamanda bilgi toplama veya parmakizi (fingerprinting) olarak adlandırılır ve genellikle gerçek bir giriş ve DoS ataklarından önce gelir.

Paket toplama yoluyla hattı dinleme (sniffing) ve kablosuz trafik gözetleme (snooping) gizli dinleme (eavesdropping) alanında kullanılan yaygın terimlerdir. Bu yöntemle toplanan bilgiler daha sonra ağa giriş ve DoS atakları için kullanılabilir [27].

Aldatma (spoofing) olarak tanımlanan yöntemle, sahte ARP bildirim mesajı yayınlarlar. Saldırılmak istenen hedef makinenin MAC adresi, paketi gönderen adres olarak yazıldığı bir sahte paketin bir yayın adresine gönderilmesiyle bu saldırı başlatılır. Bunun sonucunda yayın bölgesindeki tüm makineler hedef makineye cevap paketlerini gönderir [50]. Birçok sahte ARP mesajının gönderilmesi, ağ elemanlarının yanlış adreslere veri göndermesine neden olmakta, böylece bu mesajların bir kısmı saldırganın eline geçmektedir. Bu sayede saldırgan, seçeceği bir kurban hakkında bilgiye sahip olur. Böylece, ortadaki adam (man in the middle) saldırısı başta olmak üzere, farklı tipte saldırılar gerçekleştirilebilir. Saldırgan, ağa zarar verebileceği gibi, ağ trafiğini

izleyebilir ve ağ kullanıcılarının şifrelerini ele geçirebilir [42]. Eğer şifreleme kullanıldıysa saldırganın önce şifreyi kırması gerekir. Bu WEP tabanlı sistemlerde kolayken WPA ve RSN'de çok daha zordur [48].

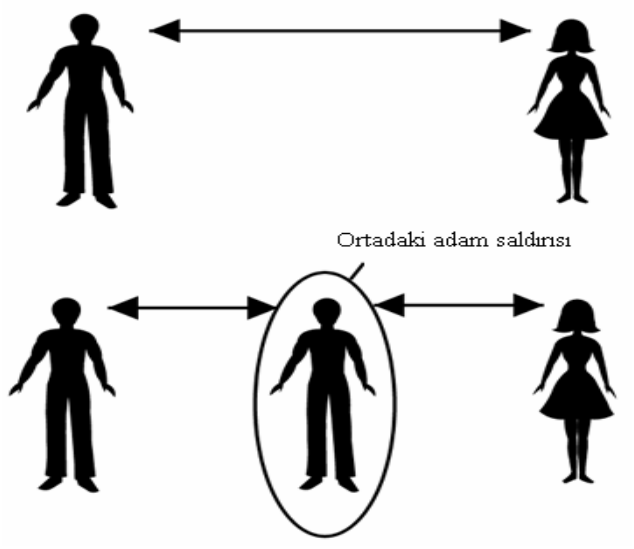
Şifreleme yöntemleriyle bu tür dinleme saldırılarına karşı önlem alınabilir.
Kablosuz dinleme ağ trafiğini gözlemlemek ve kullanımdaki SSID'leri keşfetmek, geçerli MAC adresleri veya şifreleme kullanılmışsa bunu tespit etmek için kullanılabilir [27]. Kablosuz keşif çoğunlukla war driving olarak isimlendirilmiştir. Aktif ve pasif kablosuz ağları taramak için yardımcı programlar kullanılmıştır. Hakkında ek bir bilgiyi iletirler.

3.4.1.2. Giriş Saldırıları

Sisteme giriş yetkisi olmayan kişinin sisteme girmek üzere yaptığı saldırı türüdür. Giriş ataklarına, zayıf şifreli veya şifresiz ağların istismarı, HTTP, FTP, Telnet gibi hizmetlerin istismarı örnek gösterilebilir. Davetsiz bir misafir, şifre, sunucu ve veri dosyaları gibi değerli bilgileri taşıyan organizasyon üyesine hile yapabilir. Kırma işlemi çok daha kolaylaşır. Bir saldırgan kablosuz ağ üzerinden sunucular ve istasyonlar gibi kablolu ağ bölümlerine giriş kazanmak için bir erişim noktası kullanır. Çok daha bilgili saldırganlar erişim noktasının kontrolünü almak için uğraşırlar ve eğer gerekli ise ayarlarını değiştirirler.

Çoğu istemci yüksek sinyal gönderen erişim noktasıyla bağlantı kurmaya çalışır. Hilekâr (rogue) AP olarak bilinen yetkisiz bir erişim noktası, güçlü sinyal verdiğinde istemciler bu cihazla ilişkiye geçmeye çalışacaktır. Hilekâr erişim noktası ağ üzerindeki cihazlarla iletişim kurabilir. Böylece hilekâr erişim noktası ortadaki adam durumuna girip şifrelenmiş bir ortama girme hakkı kazanacaktır [27].

Ortadaki adam saldırılarında saldırgan iki nokta arasındaki iletişimi keserek, iletişim noktasından birini taklit eder ve diğer istemciyle bilgi alışverişine girer. Dinlediği ağdan elde ettiği paketten mesaj doğruluğunu belirleyen veriyi bozarak 2 nokta arasındaki iletişimi koparır. Yetkilendirilmiş kullanıcın paketleriyle kendini erişim noktasına doğrulatabilir [48].



Şekil 3.20: Ortadaki adam saldırısında saldırganın durumu

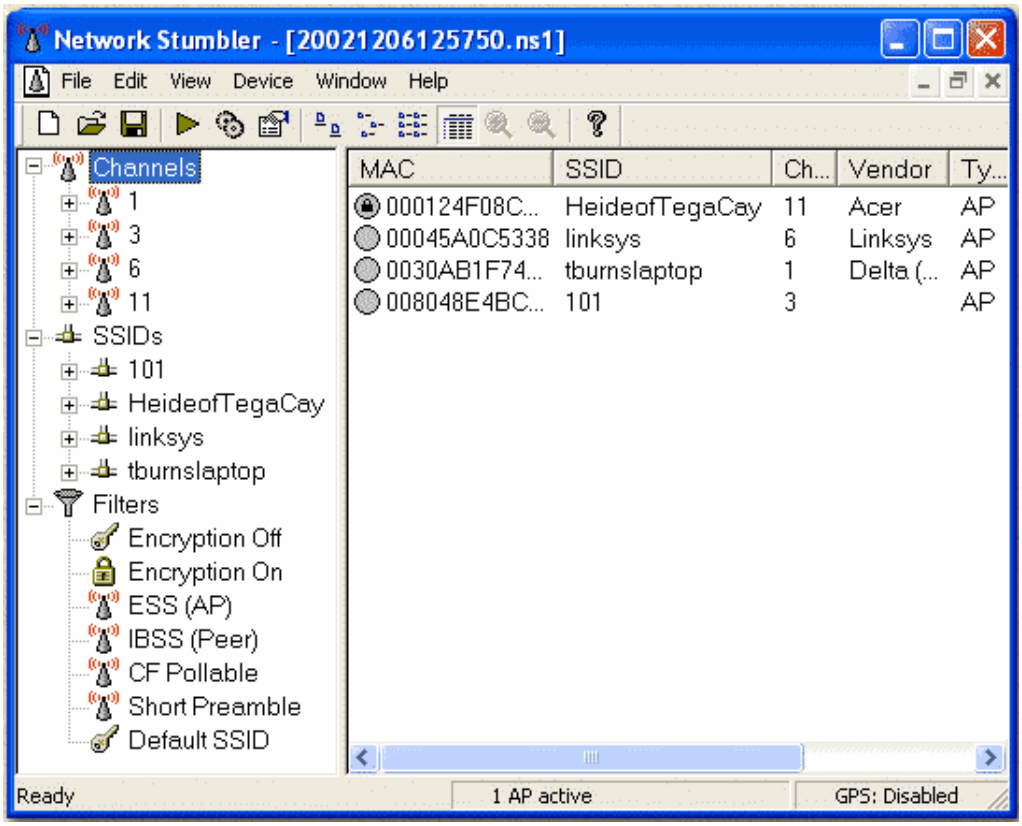
3.4.1.3. Hizmeti Engelleme Saldırıları (DoS-Denial of Service)

Bir saldırganın kablosuz ağları, sistemleri veya hizmetleri kullanıcıların erişemeyeceği duruma getirmesine hizmeti engelleme saldırıları denir. DoS atakları birçok şekilde olabilir. Çoğu kez saldırı sırasında bir script, otomatikleştirilmiş bir aracın kullanılmasıyla gerçekleşir. Yüksek harap etme potansiyeli nedeniyle DoS saldırıları önlenmesi son derece zor olduğundan çok korkulan saldırı türüdür.

Saldırgan, programlar yardımıyla ilişkilendirilmemiş sahte paketler göndererek 802.11 istemcilerinin erişim noktasından kopmasına sebep olur. Bu saldırı programları çalıştığı sürece istemci kablosuz ağı kullanamaz. 2.4 veya 5 Ghz'de çalışan her aygıt sinyal boğmak üzere bir DoS saldırı aracı olarak kullanılabilir. Kablosuz boğma ya da engel kablosuz ağlarda çözülmemiş öncelikli güvenlik konusudur. Basit bir boğma aktarıcısı iletişimi imkânsız hale getirir. Sürekli giriş isteğiyle erişim noktasının meşgul edilmesinden dolayı erişim noktası isteklere cevap veremez hale gelir.

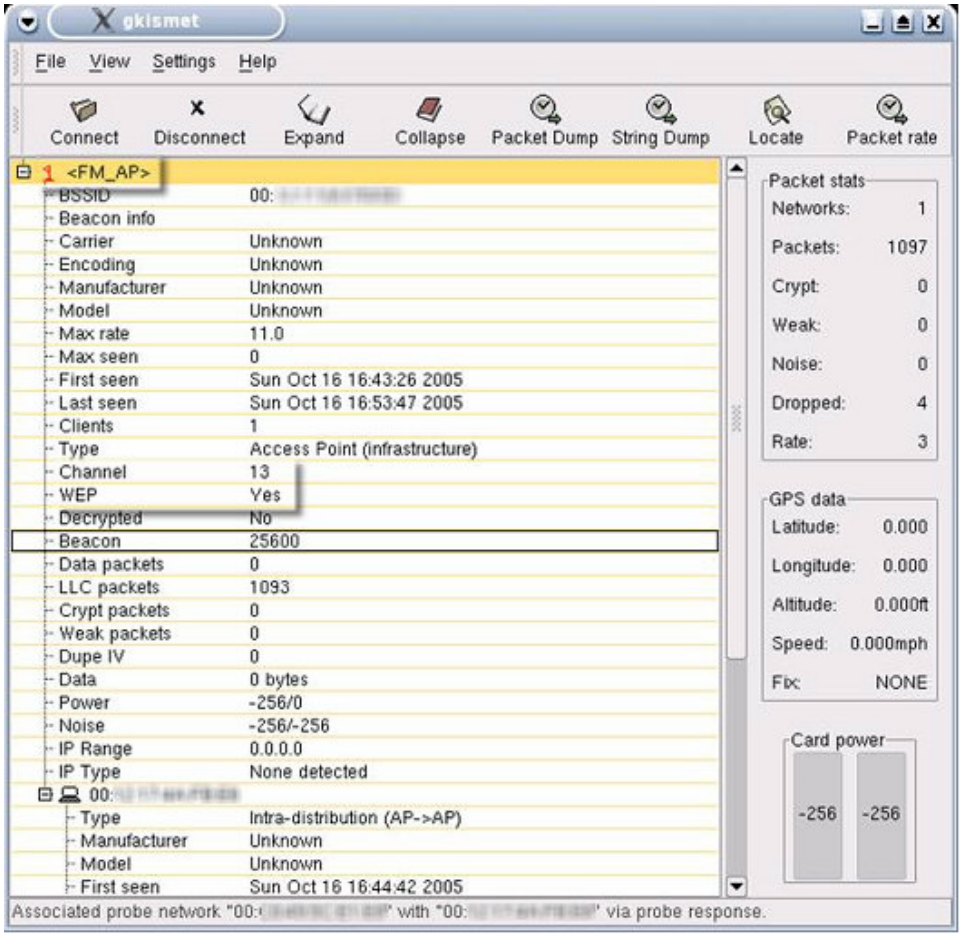
3.4.2. Saldırı Araçları

Netstumbler: Windows altında çalışan war driving araçlarından biridir. Civardaki erişim noktalarını bulmak için kullanılır. Netstumbler, bir aktif tarayıcıdır, araştırma sırasında civara araştırma istekleri gönderir, dolayısıyla tespit edilebilir [51].



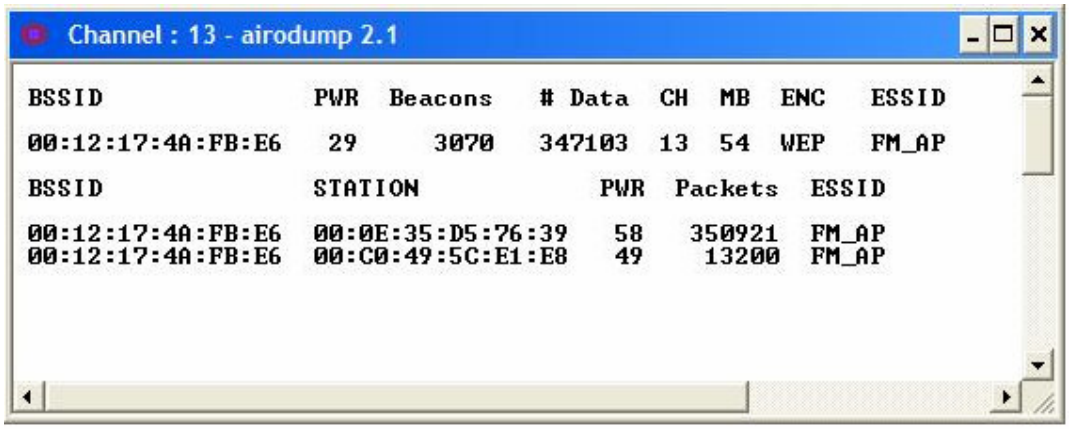
Şekil 3.21: Çalışan bir Netstumbler penceresi

Kismet: Pasif bir tarayıcıdır SSID yayınlamayan erişim noktalarını bulabilir. Kendini belli etmeyen bu erişim noktalarını ilk adımda trafiklerinden tespit eder. İlk adımda SSID'sini bulamadığı erişim noktasını daha sonra SSID içeren ilk paketi gördüğünde bulabilir. Ayrıca paket toplama ve bağlanan istemcileri görmeniz mümkündür Kismet gibi pasif araçlar kablosuz ağda tarama yaparken bilgi taşımazlar [27, 52].

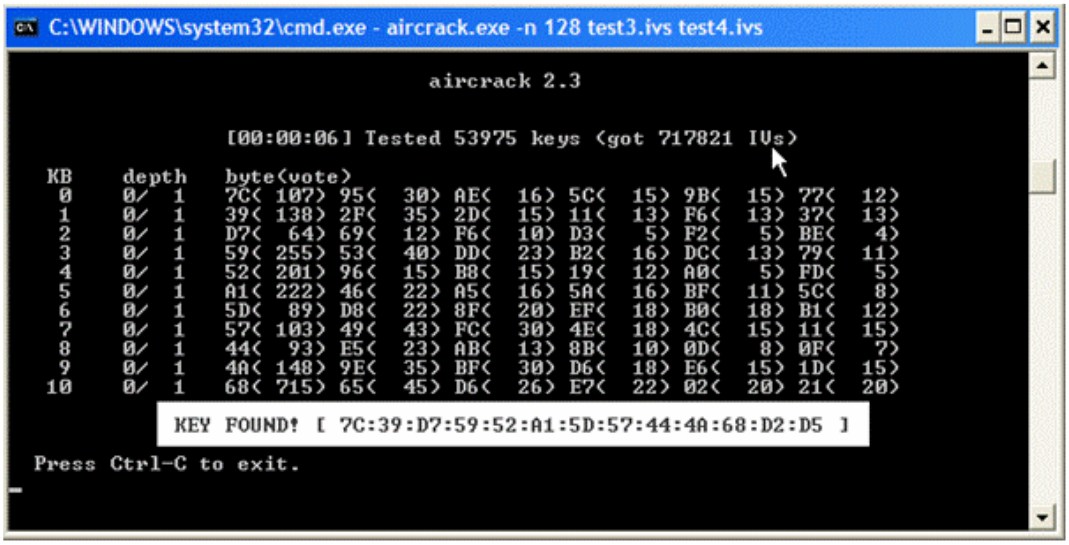


Şekil 3.22: Kismet çalışma penceresi

Airodump: Kablosuz ağda IV paketlerini toplamak için kullanılır, yeterince IV toplandığında Aircrack programı ile WEP anahtarlarını çözmek mümkündür [53].

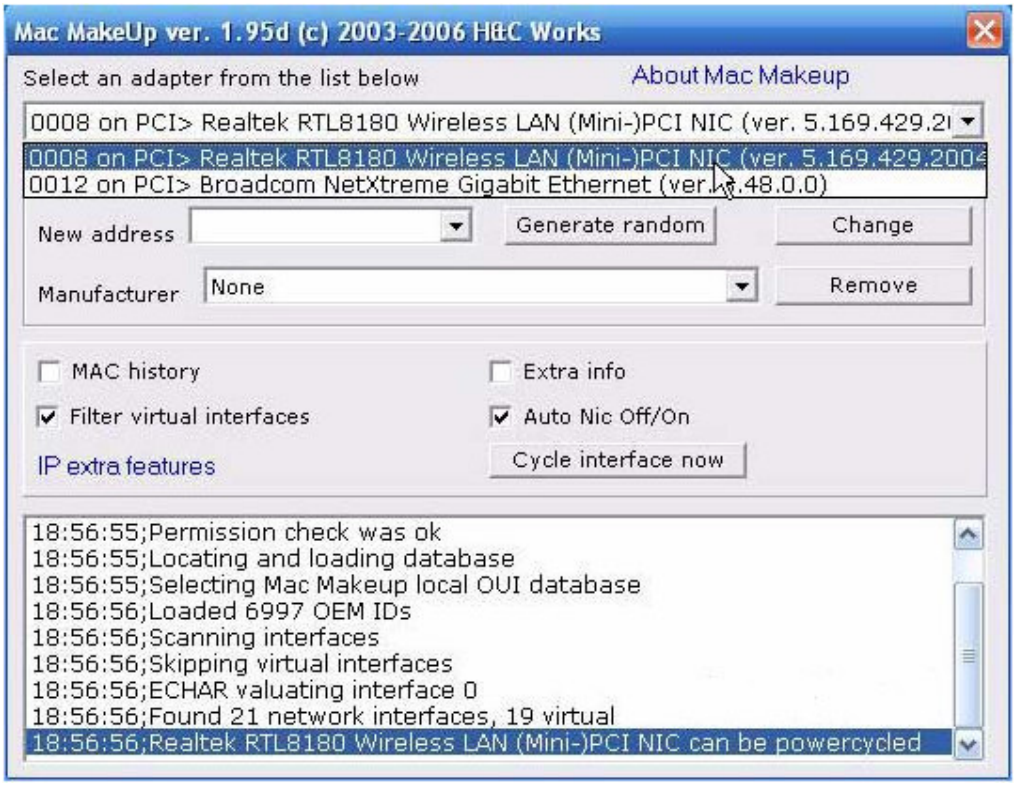


Şekil 3.23: Airodump ile paket toplama



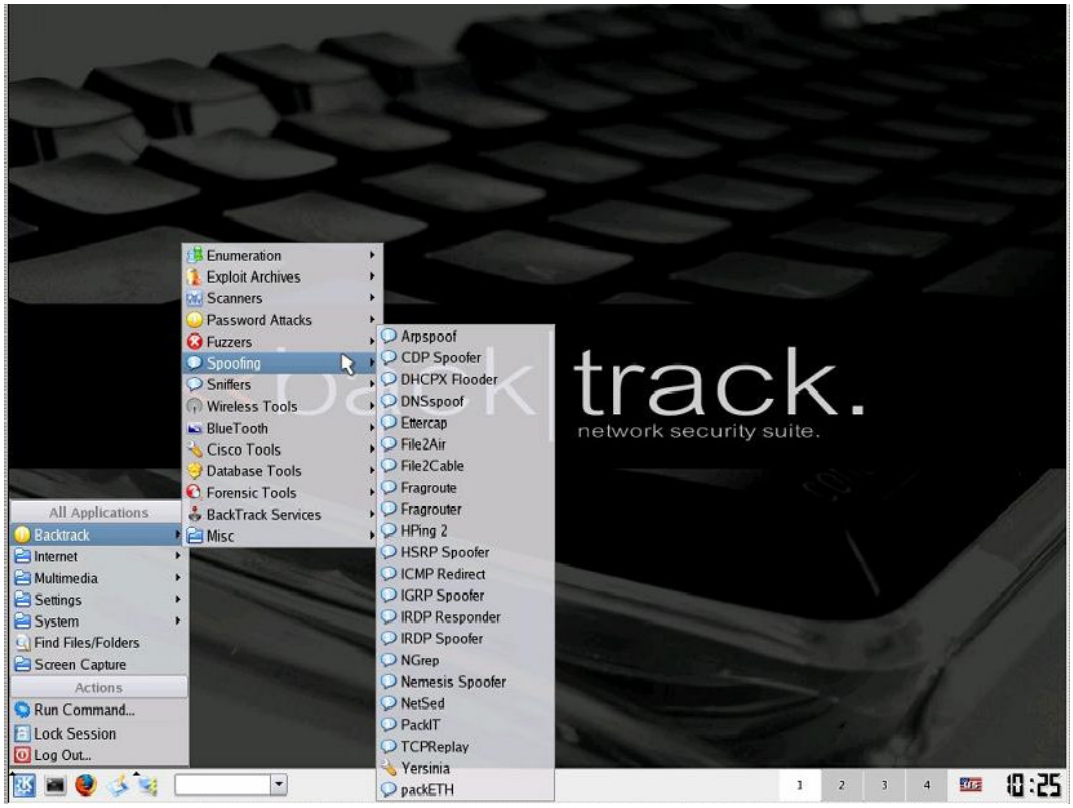
Şekil 3.24: Aircrack ile 128 bit şifrenin çözülmesi

Mac Makeup: MAC adresini değiştirmeye yarayan basit bir programdır. Geçerli MAC adresini istenilen şekilde yenisi ile değiştirmede kullanılır [25].



Şekil 3.25: Mac Makeup ile MAC adresini değiştirme

Backtrack: Güvenlik denetim uzmanları tarafından kullanılması amacıyla tasarlanmış, içinde birçok araç bulunduran bir dağıtımdır [54].



Şekil 3.26: Backtrack program grubu

4. SONUÇ

Kablosuz ağların ortaya çıkmasından beri bu alandaki teknolojik ilerleme çok büyük olmuştur. Ancak teknolojik ilerlemeyle birlikte güvenlik savunmasızlıkları da ortaya çıkmıştır. Yapılan iyileştirme çalışmalarında yeni güvenlik standartları oluşturulmuştur. İlk nesil kablosuz ağlar güvenliği seçenekli olarak tanımlamıştır, yeni nesil güvenlik protokolleri ise kablosuz ağlara girişte doğrulamayı zorunlu hale getirmiştir. Şifreleme algoritmaları geliştirilerek kablosuz ağa izinsiz girişler engellenmeye çalışılmıştır.

Kablosuz ağların çalışma biçimi Ethernet teknolojisinde kullanılan CSMA/CD tekniği ile karıştırılmamalıdır. CSMA/CD ile paket çarpışmaları kontrol edilir ve düzenlenir. Kablosuz ağların kullandığı CSMA/CA ise çarpışma duyduğunda ağdaki aygıtlara hiçbir bilgiyi yayınlamamalarını söyler. Kablolu ağlarda 3. katman üzerinde çalışan güvenlik duvarı ve saldırı tespit sistemleri kablosuz ağlarda güvenliği sağlayamaz. Kablosuz ağ güvenliği 2. katman problemidir.

Bu raporda tartışılan tüm yöntemlerin kendi hata payları ve sınırlılıkları vardır. Genişletilebilir doğrulama protokolünde kullanılan yöntemlerin birçoğu halen yayılmakta ya da yayılma sürecindedirler. Halen yayılmakta olan iki ana yöntem kümemiz bulunmaktadır. Bunlar sertifikaya dayalı ve şifreye dayalı yöntemlerdir. Daha çok kullanıcı yanlısı olan şifreye dayalı yöntemler bireysel kullanıcılar için daha uygunken yayılmaları ve yönetimsel yükler pahasına daha fazla güvenlik sağlayan sertifikaya dayalı yöntemler ise büyük firmalar ve girişimlerce tercih edilmektedir. Farklı koşullarda uygulanabilmeye elverişli olmalarının yanı sıra bu yöntemler birlikte işlerlik konularında çeşitli engellerle karşılaşırlar.

Kablosuz anahtarlar kullanılarak erişim noktalarını merkezi olarak yönetebilmek mümkündür. Bu cihazlar ile erişimler kontrol edilebilir, güvenlik yapılanması oluşturulabilir, kullanımlar izlenebilir. Bu yollarla hilekâr erişim noktalarını tespit etmek kolaylaşır. Merkezi kontrol ile kablosuz ağın sorunsuz kullanılması sağlanır.

Cihazların varsayılan ayarları değiştirilmelidir. Donanımın fabrika çıkış ayarında herkes tarafından bilinen ya da üretici firmanın internet sitesinde kolaylıkla bulunabilecek yönetici şifresi ve SSID tanımı vardır. Varsayılan şifreleri bilen yetkisiz kişiler kablosuz ağın yönetimini ele geçirebilmektedir. Erişim noktasının yönetici şifresi değiştirilerek bu noktada önlem alınmalıdır. Varsayılan SSID tanımı değiştirilerek yayını kapatılmalıdır. Varsayılan SSID kullanıldığı durumda erişim noktasının marka ve modeli hakkında saldırgan bilgi sahibi olmaktadır. Donanımın açık noktalarını bilen saldırganın kablosuz ağa ulaşması daha kolay olacaktır. SSID yayını kapatılarak dileyen herkes tarafından kablosuz ağın görülmesi engellenecektir. Kablosuz ağa erişecek kimseleri daha iyi kontrol etmek için MAC adres filtrelemesi etkinleştirilmelidir. Erişim noktalarına izin verilen MAC adresleri listesi tanımlanmalıdır. Alınan bu basit önlemler ile temel bir koruma oluşturulmalıdır.

Ağ trafiğinin güvenliği güçlü bir protokol ile sağlanmalıdır. Kurumsal bağlantılarda, ihtiyaçlar ve olanaklar çerçevesinde uygun bir doğrulama protokolü seçilmelidir. Erişim noktaları güvenlik duvarının önüne kurulmalı, kablolu ağa erişecek kullanıcılar erişim noktasına bağlanarak güvenlik duvarından şirket ağına sanal özel ağ ile erişmelidir. Bu erişim sağlanırken istemci, RADIUS sunucusu tarafından doğrulanmalıdır. RADIUS sunucusu güvenlik duvarı arkasında olmalıdır. Farklı erişim noktaları kullanılarak kullanıcı seviyesi ve misafir kullanıcı seviyesi olan kablosuz ağlar tanımlanmalıdır. Sanal özel ağlar ile bu grupların kablolu ağa erişimleri tanımlanmalıdır.

KAYNAKLAR

1. ERARSLAN, E. , *Akademik çalışmalar*, Başkent Üniversitesi, http://www.baskent.edu.tr/~eraslan/index2.htm [Ziyaret Tarihi: Ocak 2007].

2. PUSULA NET KURUMSAL HİZMETLER, *Yerel alan ağ hizmetleri*, http://www.pusula.net.tr/yerelag.htm [Ziyaret Tarihi: Ocak 2007].

3. KARACI, A. , *İnternetle ilgili bazı temel kavramlar,* Gazi Üniversitesi, http://w3.gazi.edu.tr/web/akaraci/ders/internet.htm [Ziyaret Tarihi: Şubat 2007].

4. ÇAĞILTAY, K. , 1994, *Herkes için internet*, Ankara Üniversitesi, http://bid.ankara.edu.tr/start/hii [Ziyaret Tarihi: Şubat 2007].

5. ŞENGONCA, H. , *Prof. Dr. Halil SENGONCA,* Ege Üniversitesi, http://bornova.ege.edu.tr/~sengonca/cscomp1.doc [Ziyaret Tarihi: Mart 2007].

6. ODOM, W. , 2003, *Cisco CCNA 640–647 sınavı sertifikasyon rehberi*, Sistem Yayıncılık, İstanbul, 975–322–301–3.

7. KAPLAN Y. , 2000, *Veri haberleşmesi temelleri*, Papatya Yayınları, İstanbul, 975–6797–15–0.

8. TANRISEVER, T. , *LAN-Ethernet*, Balıkesir Üniversitesi, http://stream.balikesir.edu.tr/~taner/networking/bilgisayar_aglari/LAN-Ethernet.htm [Ziyaret Tarihi: Mart 2007].

9. CISCO NETWORK ACADEMY, *CCNA 1: Networking basics v.3.1.1.* , http://curriculum.netacad.net [Ziyaret Tarihi: Mart 2007].

10. 10. CISCO SYSTEMS DOCUMENTATON, *Internetworking technology handbook*, http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ethernet.htm [Ziyaret Tarihi: Mart 2007].

11. KAPTAN, H. , *Yerel alan ağları*, Marmara Üniversitesi, http://mimoza.marmara.edu.tr/~hkaptan/lan.htm [Ziyaret Tarihi: Mart 2007].

12. OKTUĞ, S. , 2006, *BLG433-Bilgisayar haberleşmesi* ders notları, İstanbul Teknik Üniversitesi, http://www3.itu.edu.tr/~oktug/BH/notlar/bolum4.pdf [Ziyaret Tarihi: Mart 2007].

13. HERNANDEZ, L. , *Back to basics: LAN technologies,* Agilent Technologies Network Resources White Paper, http://literature.agilent.com/litwebpdf/5968-1060E.pdf [Ziyaret Tarihi: Nisan 2007].

14. ÇÖLKESEN, R. , 2001, *Network TCP/IP unix el kitabı,* Papatya Yayınları, İstanbul, 975–6797–02–9.

15. GNU/LINUX DOCUMENTATION PROJECTS, *Network,* İnönü Üniversitesi, http://stu.inonu.edu.tr/~helkirmizi/network.htm [Ziyaret Tarihi: Nisan 2007].

16. TECHFEST, *Ethernet technical summary - Chapter 2,* http://www.techfest.com/networking/lan/ethernet2.htm [Ziyaret Tarihi: Nisan 2007].

17. BUYAMER, 2006, *Bilgisayar bilimleri uygulama ve araştırma merkezi*, İstanbul Üniversitesi, http://buyamer.istanbul.edu.tr/index.asp?grp=egitim&no=14 [Ziyaret Tarihi: Nisan 2007].

18. BLANK, Andrew G. , 2004, *TCP/IP foundations,* Alameda, CA, USA: Sybex, Incorporated, http://site.ebrary.com/lib/bahcesehir/Doc?id=10131879&ppg=72 [Ziyaret Tarihi: Nisan 2007].

19. SALAHLI, V. , 2003, *Transmission control protocol,* http://www.enderunix.org/docs/tcpip/tcp/tcp.html [Ziyaret Tarihi: Nisan 2007].

20. TÜRKER, İ. , 2003, *User datagram protocol*, http://www.enderunix.org/docs/tcpip/udp/udp.htm [Ziyaret Tarihi: Nisan 2007].

21. AYAV, T. , YILMAZ, S. , 2003, Bir ağ yönetim sistemi: Guardilan, *TBD 20th Bilisim Kurultayi Bildiriler Kitabi*, Eylul 2003, İstanbul, 1–1.

22. INDEX of VERİ İLETİŞİM MODELLERİ, 2005, *ICMP*, Hacettepe Üniversitesi, http://ogrenci.hacettepe.edu.tr/~b0045188/veri_iletisim_modelleri/html_dosyalar/icmp.htm [Ziyaret Tarihi: Nisan 2007].

23. ARKIN, O. , 2001, *ICMP usage in scanning*, The Sys-Security Group, http://www.sys-security.com/archive/papers/ICMP_Scanning_v3.0.pdf [Ziyaret Tarihi: Nisan 2007].

24. ÇAY, K. , 2006, *TCP / IP protokol grubu tarihçesi,* http://www.turkcenet.org/index.php?option=com_content&task=view&id=256&Itemid=55&limit=1&limitstart=1 [Ziyaret Tarihi: Nisan 2007].

25. KINDERVAG, J, 2006, The five myths of wireless security, *Telecommunication And Network Security*, September-October, 7-16.

26. MICROSOFT-TECHNET, 2007, *Kablosuz ağ kavramları*, http://www.microsoft.com/technet/prodtechnol/windowsserver2003/tr/library/ServerHelp/fbf4ab12-723a-4c53-bcdd-01cabe9d7b87.mspx?mfr=true [Ziyaret Tarihi: Nisan 2007].

27. CISCO NETWORKING ACADEMY PROGRAM, 2004, *Fundamentals of wireless LANs companion guide*, Cisco Press, USA, 1–58713–119–6.

28. YILMAZ, M. S. ,2002, *CISN*, Ortadoğu Teknik Üniversitesi, http://cisn.odtu.edu.tr/2002-6/ieee.php [Ziyaret Tarihi: Mayıs 2007].

29. ODTÜ - BİDB: *Network grubu*, 2007, http://www.bidb.odtu.edu.tr/index.php?go=ng&sub=802_11_b [Ziyaret Tarihi: Mayıs 2007].

30. BAĞLAN BİLGİSAYAR, 2005, *Bluetooth sıkça sorulan sorular,* http://www.baglan.com.tr/urunler/brainboxes/bluetooth_faq.html [Ziyaret Tarihi: Mayıs 2007].

31. ÖZDEMİR, M. , 2003, *Kablosuz yerel ağ teknolojileri,* Bitirme tezi, Kocaeli Üniversitesi.

32. IEEE STANDARDS FOR INFORMATION TECHNOLOGY, *IEEE-SA GetIEEE 802.11 LAN/MAN wireless LANS*, 2006, http://standards.ieee.org/getieee802/802.11.html [Ziyaret Tarihi: Mayıs 2007].

33. ZAHARIADIS, T. , 2004, *Evolution of the wireless PAN and LAN standards*, Computer Standards & Interfaces, 26, 175–185.

34. TÜFEKÇİOĞLU, F. , 2005, *Hareket bilinçli, güvenilir tasarsız ağ yönlendirme protokolleri*, Yüksek lisans tezi, İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü.

35. ŞEN, Ö. F. , *Wireless network,* http://www.enderunix.org/docs/kablosuz_alan_aglari [Ziyaret Tarihi: Mayıs 2007].

36. GÜRKAŞ, G.Z. , DURUKAN, Ş. , ZAİM, A.H. , DEMİR, A. , AYDIN, M.A. , 2005, 802.11b Kablosuz ağlarda güvenliğin ağ trafiği üzerindeki etkilerinin analizi, *II. Mühendislik Bilimleri Genç Araştırmacılar Kongresi,* 17–19 Kasım 2005, İstanbul, 975–404–758–8, 8–15.

37. DANTU, R. , GABRIEL, C. , ATRI, A. , 2007, EAP methods for wireless networks, *Computer Standards & Interfaces*, 29, 289–301

38. ARBAUGH, W. A. , SHANKAR, N. , WAN, Y. C. , 2002, Your 802.11 Wireless network has no clothes, *Wireless Communications, IEEE [Personal Communications],* 9, 44-51.

39. DEMİREL, İ. Ö. , ÖRENCİK B. , 2005, *Ağ güvenliği dersi-Telsiz ağ güvenliği*, İstanbul Teknik Üniversitesi, http://www3.itu.edu.tr/~orencik/Ag_Guvenligi_Dersi.html, [Ziyaret Tarihi: Mayıs 2007].

40. MANLEY, M. E. , McENTEE C. A. , MOLET, M. A. , PARK, S. J. , 2005, Wireless security policy development for sensitive organizations, *Systems, Man and Cybernetics (SMC) Information Assurance Workshop, 2005. Proceedings from the Sixth Annual IEEE*, 15–17 Haziran 2005, 150 – 157

41. CISCO SYSTEMS DOCUMENTATON, *A comprehensive review of 802.11 wireless LAN security and the Cisco wireless security suite*, http://www.cisco.com/en/US/products/hw/wireless/ps430/products_white_paper09186a00800b469f.shtml, [Ziyaret Tarihi: Mayıs 2007].

42. YÜKSEL, E. , SOYTÜRK, M. , OVATMAN, T. , ÖRENCİK, B. , *Telsiz yerel alan ağlarında güvenlik sorunu*, http://www.emo.org.tr/resimler/etkinlikbildirileri/3634c1dcbe056c1_ek.pdf, [Ziyaret Tarihi: Mayıs 2007].

43. TEPUM SECURA, 2004, *Kablosuz ağlarda güvenlik*, http://www.tepum.com.tr/Etkinlikler/**Kablosuz**AglardaGuvenlik.pdf, [Ziyaret Tarihi: Mayıs 2007].

44. *Kerberos V: The network authentication protocol*, Massachusetts Institute of Technology, http://web.mit.edu/Kerberos, [Ziyaret Tarihi: Mayıs 2007].

45. MICROSOFT, 2006, *Windows XP'de WPA kablosuz güvenlik güncelleştirmesine genel bakış*, http://support.microsoft.com/kb/815485/tr, [Ziyaret Tarihi: Mayıs 2007].

46. MICROSOFT-TECHNET, 2005, *Kablosuz ağlar için güvenlik bilgileri*, http://technet2.microsoft.com/WindowsServer/tr/Library/ff7c2ac9-5db3-4b71-a31b-9604dce0b2171055.mspx?mfr=true, [Ziyaret Tarihi: Mayıs 2007].

47. ITU / BIDB, *WPA-WPA2*, http://www.bidb.itu.edu.tr/?d=468, [Ziyaret Tarihi: Mayıs 2007].

48. ARBAUGH, W. A. , EDNEY, J. , 2003, *Real 802.11 security: Wi-fi protected access and 802.11i,* Addison Wesley, 0–321–13620–9

49. KABAL, O. , 2005, *802.1x port tabanlı kimlik kanıtlama nasıl,* http://www.belgeler.org/howto/p8021x-howto.html , [Ziyaret Tarihi: Haziran 2007].

50. CANBERK, G. , SAĞIROĞLU, Ş. , 2006, Bilgi ve bilgisayar güvenliği casus yazılımlar ve korunma yöntemleri, Grafiker Ltd. Şti. , Ankara, 975-6355-26-3.

51. 2007, *NETSTUMBLER*, http://www.netstumbler.com, [Ziyaret Tarihi: Haziran 2007].

52. KERSHAW, M. , 2007, *Kismet*, http://www.kismetwireless.net, [Ziyaret Tarihi: Haziran 2007].

53. 2006, *Airodump Main,* *h*ttp://www.wirelessdefence.org/Contents/Aircrack_airodump.htm, [Ziyaret Tarihi: Haziran 2007].

54. MOSER, M. , *Remote-Exploit.org - Supplying offensive security products to the world,* http://www.remote-exploit.org/backtrack.html, [Ziyaret Tarihi: Haziran 2007].