KARADENİZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ ANABİLİM DALI

KABLOSUZ YEREL ALAN AĞLARINDA(WLAN) GÜVENLİK UYGULAMALARI VE SES HABERLEŞMESİ(VoIP)

YÜKSEK LİSANS TEZİ

Elektrik-Elektronik Müh. Soner KADAKOĞLU

KASIM 2010
TRABZON

KARADENİZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ ANABİLİM DALI

KABLOSUZ YEREL ALAN AĞLARINDA(WLAN) GÜVENLİK UYGULAMALARI VE SES HABERLEŞMESİ(VoIP)

Elektrik-Elektronik Mühendisi Soner KADAKOĞLU

Karadeniz Teknik Üniversitesi Fen Bilimleri Enstitüsünce
"Elektronik Yüksek Mühendisi"
Unvanı Verilmesi İçin Kabul Edilen Tezdir.

Tezin Enstitüye Verildiği Tarih : 15.10.2010
Tezin Savunma Tarihi : 04.11.2010

Tez Danışmanı : Yrd. Doç. Dr. İsmail KAYA
Jüri Üyesi : Yrd. Doç. Dr. Ali ÖZEN
Jüri Üyesi : Yrd. Doç. Dr. Hüseyin PEHLİVAN

Enstitü Müdürü : Prof. Dr. Salih TERZİOĞLU

Trabzon 2010

ÖNSÖZ

Kablosuz Yerel Alan Ağları sağladığı kolay kurulum, kolay genişletilebilirlik, gezginlik gibi avantajlarıyla günümüzde hızla büyümekte ve özellikle iş dünyasında ve bilgisayar sektöründe popülerliği artmaktadır. Gelişen teknoloji, artan aktarım hızları ve üreticiler arası gidilen standardizasyon çalışmalarıyla her geçen gün daha fazla uygulama alanı bulmakta ve kullanıcı sayısı artmaktadır. Bu uygulamalardan biri de kablosuz ip telefon üzerinden haberleşmedir. Bu çalışmada kablosuz IP telefonlarla yapılan haberleşmenin deşifre edilmemesi için kablosuz ağın hem en güvenilir hem de en kaliteli nasıl olacağı incelenmiştir.

Bu tezi hazırlarken desteklerinden ötürü Danışman Hocam Sayın Yrd. Doç. Dr. İsmail KAYA'ya, Saygıdeğer iş arkadaşlarıma, Saygıdeğer TÜRK TELEKOM A.Ş.'ye ve maddi manevi her türlü destekleriyle yanımda olan Saygıdeğer aileme teşekkürlerim daim olsun isterim.

Soner KADAKOĞLU
Trabzon 2010

İÇİNDEKİLER

ÖZET

Kablosuz Yerel Alan Ağları sağladığı kolay kurulum, kolay genişletilebilirlik, gezginlik gibi avantajlarıyla günümüzde hızla büyümekte ve özellikle iş dünyasında ve bilgisayar sektöründe popülerliği artmaktadır. Gelişen teknoloji, artan aktarım hızları ve üreticiler arası gidilen standardizasyon çalışmalarıyla her geçen gün daha fazla uygulama alanı bulmakta ve kullanıcı sayısı artmaktadır.

Kablosuz Yerel Alan Ağları (Kablosuz LAN) için kullanılan standartlar IEEE(Institute of Electrical and Electronic Engineers) tarafından geliştirilen 802.11 standardıdır. Bu standartların gelişimi 1997 yılında 802.11 ile başlamıştır. 1999 yılında 802.11b ve 802.11a, 2003 yılında da 802.11g ve 2008 yılında da 802.11n standart haline gelmiştir. 802.11i ise var olan 802.11 standartları üzerinde güvenlik iyileştirmelerini içermektedir[21].

Kablosuz Yerel Alan Ağları sistemlerinde ilk nesil güvenlik protokolü WEP (Wired Equivalent Privacy)'tir. Şifreleme algoritması olarak RSA Data Security tarafından geliştirilen RC4 algoritmasını kullanır. WEP'in birçok güvenlik açığı tespit edilmiştir. Bu güvenlik açıklarını gidermek için ikinci nesil güvenlik protokolü 802.11i geliştirilmeye başlanmıştır fakat kısa vadede bir ara çözüm sağlayabilmek için Wi-Fi Protected Access (WPA) adlı sistem ortaya çıkmıştır. WPA'da TKIP (Temporal Key Integrity Protocol) protokolü WEP'e bir güncelleme olarak tasarlanmıştır. 802.11i WEP ve TKIP'ın yerini alması için CBC-CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol) protokolünü tanımlamaktadır[12]. Bu sistem şifreleme algoritması olarak AES (Advanced Encryption Standart)'i kullanır[12].

Bu tez de 802.11g standardında çalışan bir erişim noktası ile kurulan bir Kablosuz Yerel Alan Ağında öncelikle WEP güvenlik protokolünü kullanarak bir kablosuz ip telefon ile bir kablolu ip telefon arasındaki ses veri akışı incelenmiştir. Daha sonra WPA güvenlik protokolü kullanılarak bir kablosuz ip telefon ile bir kablolu ip telefon arasındaki ses veri akışı incelenmiştir. WPA güvenlik protokolü ile kayıplar oluşmadan ses veri akışının nasıl elde edileceği irdelenmiştir.

Anahtar kelimesi: WLAN, LWAPP, WEP, WPA, Voice over IP,

SUMMARY

VOICE COMMUNICATION (VoIP) AND SECURITY APPLICATION ON WIRELESS LOCAL AREA NETWORK

The wireless lan grows rapidly nowadays with the advantages such as easy installation, widening and moving ,its popularity increases especially in business world and computer sector. With the help of developing technology, rising transfer rate and standardization labouring among the manufacturers,they find more application fields day by day and the number of users increases.

The standards used for the wireless lan are 802.11 ones developed by IEEE(Institute of Electrical and Electronic Engineers).The developments of these standards started in 1997 with 802.11.It became 802.11b and 802.11a in 1999, 802.11g in 2003 and 802.11n in 2008. 802.11i involves security redevelopment of the existent 802.11.

On the wireless lan the first generation security protocol is WEP(Wired Equivalent Privacy). RC4 algorithm developed by RSA Data Security is used as a coding algorithm.Many security deficits of WEP are ascertained.It is started to develop the second generation security protocol 802.11i in order to remove these security deficits;however, a system called Wi-Fi Protected Access appears so as to provide a short term solution. TKIP(Temporal Key Integrity Protocol) protocol on WPA is framed as an update to WEP. 802.11i defines CBC-CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol) in order to supersede WEP and TKIP.This system uses AES(Advanced Encryption Standart) as a coding algorithim.

On this thesis sound data flow between two wireless line and telephone is investigated firstly using WEP security protocol on the wireless lan installed with the hotspot run in 802.11g standard.Then the same process is looked over again by using WPA security protocol.How to get sound data flow with WPA security protocol without any loss is explicated.

Key words: WLAN, LWAPP, WEP, WPA, Voice over IP

ŞEKİLLER DİZİNİ

Sayfa No

TABLOLAR DİZİNİ

Sayfa No

SEMBOLLER DİZİNİ

AAA : Authentication, Authorization Accounting

ACL : Access Control List

AES : Advanced Encryption Standart

AP : Access Point

ARP : Address Resolution Protocol

BSS : Basic Service Set

CBC-CCMP : Counter Mode Cipher Block Chaining Message Authentication Code Protocol

CCSS : Common Chanel Signaling System

CRC : Checksum

DES : Data Encryption Standart

DKE : Dynamic Key Exchange

DNS : Domain Name System

EAP : Extensible Authentication Protocol

FIPS :Federal Information Processing Standart

FIPS : Federal Information Processing Standart

FTP : File Transfer Protocol

GHz : Giga herz

GSM : Global System for Mobile Communication

HTTP : HyperText Transfer Protocol

IBSS : Independent BSS

ICMP : Internet Control Messağe Protocol

IEEE : Institute of Electrical and Electronic Engineers

IGMP : Internet Group Management Protocol

IP : Internet Protocol

IPX/SPX : Internet Packet Exchange/Sequenced Packet Exchange

ISO : International Standards Organization

ITU :International Telecommunication Union
LAN : Local Area Network
LEAP : Lightweight EAP
LLC : Logical Link Conrol
LMDS : Local Multipoint Distribution Service
LWAPP : Light Weight Access Point Protocol
MAC : Media Access Control
Mbps : Megabit per seconds
MC :Multipoint Controller
MCU :Multipoint Control Unit
MD5 : Message Digest 5
MIB : Management İnformation Base
MIB : Management Information Base
MIC : Message Integrity Code
MP :Multipoint Processor
NIC : Network Interface Card
NIST : National Institute of Standarts and Technology
OSI : Open Systems Interconnection
PPTP : Point to Point Tunneling Protocol
PRNG : Pseudorandom Number Generator
PSTN :Public Switched Telephone Network
RC4 : Rivest Cipher 4
RF : Radio Frequency
RLAN : Radio Local Area Networks
RSA : Rivest, Shamir, Adleman , Algorithm
RSN : Robust Security Network
RTCP :Real Time Control Protocol
RTP :Real Time Transport Protocol
SMTP : Simple Mail Transfer Protocol
SNMP : Simple Network Manağement Protocol
SOHO : Small Office Home Office
SSID : Service Set Identifier

TCP	: Transmission Control Protocol
TCP/IP	: Transmissions Control Protocol/Internet Protocol
TKIP	: Temporal Key Integrity Protocol
UDP	: User Datağram Protocol
VoIP	:Voice over IP
WATM	: Wireless Asynchronous Transmission Mode
WEP	: Wired Equivalent Privacy
WINS	: Windows Internet Name Service
Wi-Fi	: Wireless Fidelity
WLAN	: Kablosuz yerel alan ağları
WLC	: Wireless Lan Controller
WPA	: Wi-Fi Protected Access

1. GENEL BİLGİLER

1.1. Giriş

Bilgisayar ağlarının kullanım amacı, kaynakların ve bilginin (veri, ses, görüntü ya da video) paylaşılması ve kişiler arasında iletişimin sağlanmasıdır. Bu paylaşım ve iletişimi sağlamak, birbirinden bağımsız ya da işlevsel olabilmek için; birbirine gereksinim duyan bilgisayarlar, çeşitli yöntemlerle bağlanarak bilgisayar ağını oluşturur. Bilgisayar ağları, eldeki kaynakların etkin paylaşımını sağlayarak ve bilgi akısını hızlandırarak verimli bir iletişim ortamı sunar [6].

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

Bir kablosuz ağ; radyo teknolojisini kullanarak, veriyi hava ortamında alan ve ileten, veri haberleşme sistemidir.

Kablosuz ağlar artık ağ teknolojileri içinde çok önemli bir yer tutmaktadır. Kablosuz yerel alan ağları (WLAN), Bluetooth ve hücresel sistemler bunları izleyen güvenlik problemleri ile beraber bilgisayar ve iş endüstrisinde hızla yükselip oldukça popüler hale gelmişlerdir. Özellikle IEEE (Institute of Electrical and Electronic Engineers) tarafından geliştirilen 802.11 ağlar gibi WLAN sistemleri özel veya genel kullanıma açık ortamlarda ortak erişim ağları haline gelmektedir[18]. Hareket özgürlüğü ve uygulanmasındaki basitlik ile WLAN sistemleri iş ve ev uygulamalarında hızla popülerlik kazanmıştır.

Wi-Fi (Wireless Fidelity) olarak bilinen 802.11 standardı, IEEE (Institute of Electrical and Electronic Engineers) tarafından kablosuz yerel ağlar için geliştirilmiş bir radyo iletim standardıdır. Wi-Fi, Bluetooth teknolojisi gibi 2.4 GHz'lik spektrumda çalışır. 100 metre yarıçap menzilindeki tüm Wi-Fi uyumlu cihazlarla, 11 Mbps – 54 Mbps gibi

yüksek hızlarda veri alışverişi gerçekleştirilir. Böylece Wi-Fi kullanılan evlerde, ofislerde ve mekanlarda kablo karmaşasından kurtulup, kullanıcılara özgürce hareket imkanı verilmektedir [16].

Kablosuz ağlardaki güvenlik riskleri kablolu ağlardaki risklerle aynıdır fakat bunlara kablosuz cihazların taşınabilirliğinden kaynaklanan yeni riskler de eklenmiştir. Bu riskleri azaltmak ve iletişimin hava ortamında kontrolsüz bir şekilde gerçekleştiği WLAN sistemlerinde güvenliği sağlayabilmek için çeşitli güvenlik mekanizmaları geliştirilmiştir.

Kablosuz Yerel Alan Ağları sistemlerinde ilk nesil güvenlik protokolü WEP (Wired Equivalent Privacy)'tir. Şifreleme algoritması olarak RSA (Rivest, Shamir, Adleman, Algorithm) Data Security tarafından geliştirilen RC4 (Rivest Cipher 4) algoritmasını kullanır. WEP'in birçok güvenlik açığı tespit edilmiştir. Bu güvenlik açıklarını gidermek için ikinci nesil güvenlik protokolü 802.11i geliştirilmeye başlanmıştır fakat kısa vadede bir ara çözüm sağlayabilmek için Wi-Fi Protected Access adlı sistem ortaya çıkmıştır. WPA (Wi-Fi Protected Access)'da TKIP (Temporal Key Integrity Protocol) protokolü WEP'e bir güncelleme olarak tasarlanmıştır. 802.11i WEP ve TKIP'ın yerini alması için CBC-CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol) protokolünü tanımlamaktadır. Bu sistem şifreleme algoritması olarak AES (Advanced Encryption Standart)'i kullanır.

1.2. Bilgisayar Ağ Kavramları

Ağdaki her bilgisayar ya da çevre birimi birer düğüm, ağ üzerinde paylaşılan kaynakları bulunduran bilgisayarlar ise sunucu olarak adlandırılmaktadır.

Ağ üzerindeki bilgisayarların karşılıklı veri aktarımında bulunabilmesi, birlikte çalışabilmesi için verici ve alıcı arasında kullanılacak işaretler, veri biçimleri ve veri değerlendirme yöntemlerinin uyumunu sağlayan kurallar kümesi protokol olarak adlandırılmaktadır. Protokol, ağdaki tüm cihazların birbirleriyle nasıl iletişimde bulunacaklarını belirlemektedir [13].

Ağ üzerindeki bilgisayarların coğrafi konumlarını ve birbirleri ile iletişimde kullanacakları sıra düzenli yapıyı belirleyen bağlantı şekilleri mimari (topoloji) olarak adlandırılmaktadır.

1.3. OSI Başvuru Modeli

Bir veri paketi, network'ten bilgisayarımıza gelirken bile onlarca işlemden geçmesi gerekir. Bu işlemlerin hepsinin bir sırası vardır ve pek çoğunun yerine getirilmesi gereken yer farklıdır. Bir veri paketi bilgisayarımıza ulaştığı andan itibaren, ekranımızda bir veri olarak gözükünceye ya da bizim işlemlerimizi etkileyecek bir komut olduğu anlaşılıncaya kadar uzun bir yol kat eder. Örneğin bir veri paketinin elektriksel sinyalizasyonunun doğru olup olmadığı daha network kartında kontrol edilecektir. Ama bir veri paketinin, bize gelen bir e- postanın bir parçası olup olmadığı ya da bağlanmak istediğimiz bir Web sitesindeki bir resim dosyasının bir kısmı olup olmadığı, işletim sisteminin çeşitli kısımlarında karar verilen bir olgudur[19].

Bu uzun yolculukta pek çok protokol görev alır. Bu protokollerin bir çalışma sırası ve her birinin özellikle rol oynadığı görevler bulunuyor[19]. Örneğin birkaç protokol birlikte çalışarak bir veri paketini şifresini çözerken, bir başka seviyede veri paketlerinin hangi programa (Internet Explorer, Outlook, FTP (File Transfer Protocol) programı vb.) ait olduğuna karar veriliyordur.

Bu işlemler seviyelere ayrılmıştır. Örneğin bir veri paketinin (şifrelenmişse) şifresi çözüldükten sonra, nereden geldiğinin bulunması ya da başka bir işlem için bir başka bileşene verilmesi öngörülmüştür.

Birbiri ardına sürdürülen bu işlemler sırasında uyulması gereken kuralları ortaya koymak ve veri paketlerinin kablodan bilgisayarımıza ulaşmasını marka ve sistem bağımsız bir hale getirerek, herkese açık bir haberleşme altyapısı kurabilmek için hazırlanmış kurallara OSI (Open Systems Interconnection) referans modeli denir[19]. Bu modelin amacı, her üreticinin ürettiği network kartından hub'a, router'a, Windows'tan Unix'e, Macintosh'a tüm cihaz, sistem ve yazılımların ortak kurallar kullanarak network üzerinden haberleşmelerini sağlamaktır. Böylece şu anda kullandığımız İnternet network'ün gibi her sisteme, markaya açık network'ler geliştirilebilir. Bunu dünyanın her yanında aynı olan trafik kurallarına ya da bir ara tüm dünyadaki insanların birbiriyle rahatça konuşulması için geliştirilmiş ama kullanım alanı bulamamış Esperanto dili projesine benzetebiliriz.

OSI modeli,1984 yılında ISO (International Standards Organization - Uluslararası Standartlar Organizasyonu) tarafından oluşturulmuş bir modeldir. Hangi network protokolünün hangi kurallara bağlı olarak çalışacağının kurallarını koymak için, iki

network bileşeni arasında yapılan bilgisayar haberleşmesini, sanal olarak her birinde farklı görevler tanımlanan ve sırayla her bileşenin kendi görevini yerine getirdiğinde bir haberleşme doğuran 7 seviyeli (katmanlı) bir çalışma sekline benzetir[19].

Böylece OSI (Open Systems Interconnection) referans modeli, sistemlerin farklı protokollerle konuşsalar bile birbirlerinden haberdar olmalarını ve verilerinden anlamalarını sağlar.

1.3.1. OSI ve Çalışma Prensibi

Daha önce OSI katmanlarının var olduğunu ve her katmanda bir kısım farklı işler yapıldığını söylemiştik. Her katman, verinin bir üst ya da alt katmanda ele alınabilecek hale getirilmesi sağlanır. Bu veriler bilgisayara ulaştıkça, her katmanda işlem görerek bir üst katmana çıkarılırlar. Üst katmanda da, veri paketinin taşıdığı veriler ve bilgiler değerlendirilmeye devam edilir.

Aynı durum bir veri network'e gönderilecekse de olur. Örneğin bir arkadaşınıza göndereceğini e-posta mesajı, önce en üst seviyede bir e-posta olarak biçimlenir. Daha sonra SMTP (Simple Mail Transfer Protocol) protokolleri içerisinde hangi e-posta adresine gideceğine dair bilgi, içindeki metin ya da eklediğiniz bir dosyaya ait şekil- format bilgisi, önem ve e-postanın açılacağı yerde uyulacak protokollerin ne olacağına dair bilgiler yazılır. Ve bir alt seviyeye geçirilir. Bu seviyede, veri hangi yolla gönderileceği, ya da hangi protokolle işleneceği gibi konulara karar verilir. Bu şekilde katmanlar arasında ilerleyerek, göndereceğiniz bilgi ham veriye, yani 1'ler ve 0'lar haline dönüştürülür[20].

OSI referans modeli, 7 katmandan oluşmaktadır. Uzun süreden beri katman (layer) şeklinde tabir ettiğimiz bu modelin nerede ya da nasıl var olduğunu merak edebilirsiniz. OSI modeli, tamamen kavramsal bir yapıdır. Örneğin 1. katmanda yapılan işlemlerin bir kısmı network kartında, diğer bir kısmı da işletim sisteminizin bir kısmında yürütülüyor olabilir. Ya da başka bir katmandaki işlerin tamamı, işletim sisteminizde çalışan bir program tarafından yürütülüyor olabilir. Sonuçta OSI kavramsal bir şablondur. Bir verinin nasıl ele alınacağını ve bu işlemlerin sırasını belirler. İşlem sırasında hangi protokolün nerede görev alacağını da tanımlar. Aynı anda bir veri üzerinde onlarca protokolün gerektirdiği işlemlerin yapıldığını düşünün. Böyle bir düzensizlikte, oluşacak karışıklığın içinden çıkmak çok zor olurdu[20].

OSI katmanlarının her birinin farklı bir ya da birkaç noktada olabileceğini söylemiş ve bu konuda bazı örnekler vermiş olduk. OSI katmanlarının her biri sadece protokollerin nelere müdahale edeceğini söyleyen ve protokol yapılarını gösteren bir modeldir. Bu katmanların neler olduğu anlaşıldıkça OSI modelini daha iyi kavrayabiliriz.

1.3.2. OSI Katmanları

OSI katmanları 7 katmandan oluşur. Bu katmanlar en üsten en alta doğru:

a)Uygulama Katmanı – Katman 7 (Application Layer - Layer 7): En üstteki katmandır. Bu katman kullanıcıların kullandığı yazılımlar için, ağa ulaşmak adına ilk servisleri sağlar. Ağ üzerinde kullanacağınız bir muhasebe yazılımı, ilk önce bu katmana ulaşmalıdır (yani yazılımların bu katmandaki işleri yapan bileşenlerine ulaşarak isteğini bildirmelidir). Örneğin e-posta, dosya transferi ve veritabanı kullanımı bu katmandaki servisler ve uygulamalarla olur[19].

b) Sunum Katmanı – Katman 6 (Presentation Layer – Layer 6): Diğer bilgisayarla alınıp verilecek olan verinin formatı üzerinde karar verir. Bu seviye, her tür bilgisayarda uygulama katmanından gelen bilgileri ortak anlaşılan bir dile çevirir. Sunum katmanı, protokollerin birbirine çevrilmesi, karakterlerin ortak karakter diline (ASCII) çevrilmesi, grafik komutlarının çalıştırılmasından sorumludur[19]. Bu katman, ayrıca verilerin sıkıştırılmasından da sorumlu katmandır. Genelde, bu katmanda kullanılan sıkıştırma metotlarının çoğu Hoffman kodlama sistemine dayanır.

c) Oturum Katmanı – Katman 5 (Session Layer – Layer 5): Bu katman iletim işleminin başlatılıp, bitirilmesi için gerekli sinyalleri üretir. Örneğin siz bir e-posta göndermek istediğinizde, veri katman 7'den katman 6'ya geçer ve burada gönderileceği protokole uygun hale getirilir. Fakat gönderme işlemi ancak bu veri katman 5'e geldiğinde, katman 5'in çalışmasından sonra başlar. Gelen veriyle birlikte, katman bir iletişim kurmak için ilk sinyalleri göndermeye başlar. Bu nedenle bu katmana, hukuk davalarındaki oturum (session) tabiriyle aynı isim verilmiştir. Bu katman, iletişimin senkronizasyonundan da sorumludur[19].

d) İletim Katmanı – Katman 4 (Transport Layer – Layer 4): İletim katmanı, oturum katmanının altında fazladan bir bağlantı katmanı sağlar. İletim katmanı, veri paketlerinin hatasız gönderilmesinden sorumludur. Bu katmanda gönderilen son paketler bir tamponda

(önbellekte) tutulur. Eğer veri paketi doğru şekilde yerine ulaşmamışsa, aynı paket birkaç kez daha gönderilir. Aynı şekilde, bu katman karşı bilgisayardan aldığı verileri doğru almışsa, karşı bilgisayara onay sinyali göndermekle sorumludur. Onay sinyalini alan karşı ağ bilgisayarı, sıradaki veriyi göndermeye başlayabilir[19].

e) Ağ Katmanı – Katman 3 (Network Layer – Layer 3): İletim katmanından gelen verilerin doğru adreslere gitmesi için gerekli adreslerin ayarlanmasında ve ağdaki trafiğin minimumda tutulacağı şekilde verilerin gönderilmesinden sorumludur. Bu katman, veri paketine nereye gitmesinin gerektiğini gösteren etiketler ekler. Bu etiketler, tabii ki 1 ve 0'lar şeklindedir[19].

f) Veri Bağlantı Katmanı – Katman 2 (Data Link Layer – Layer 2): Bu katman, veri paketlerini katman 3'ten katman 1'e iletir. İletirken, veri paketlerine boş bit'ler, 1 ve 0'lar ekler. Bu sayede, bu veriler belli bir standart uzunluğa ulaşmış olurlar. Örneğin katman 3'den gelen veri paketleri 8 ya da 40 bit arasında uzunluğa sahiptir. Katman 2 bunları 64 bit'e ya da belli bir uzunluğa tamamlar. Ayrıca bu katman iletilen ve alınan veri paketlerinin doğru bir şekilde inşa edilip edilmediğini kontrol eder. Bir hata bulduğunda düzeltir ya da verinin tekrar gönderilmesini ister[19].

g) Fiziksel Katman – Katman 1 (Physical Layer – Layer 1): Bu katman, ağ kablolarının ve ağ kartlarının verilerini elektrik sinyallerine çevirmek için kullanılan bileşenleri temsil eder. Yani, bu katmanda yer alan cihaz ve programlar, yalnızca verilerin üst katmanlarda hazırlanmış ham veriyi (0 ve 1'ler), elektrik sinyali olarak göndermekle sorumludur. Eğer gerilim veya akımda bir problem olursa ya da kablo yerinden çıkmışsa, veri aktarımını dur- durur. Her elektrik sinyalinin ne kadar süre ya da verilerin hangi veri aktarım teknolojisiyle aktarılacağını belirler[19].

OSI modeli, verinin paketlenmesi, gönderilmesi ve alınması için belirgin katmanlar oluşturmuş olur. Bir katmanda birbirine benzeyen ya da ilişkili protokollerin birlikte yer alır. Her katmanda yer alan, katmana göre özelleşmiş protokoller protokol yığını (protocol stack) adını alırlar. Bu noktada önemli olan husus, bazı protokol yığınlarının artık standart olarak kabul edilmesidir. Örneğin, TCP/IP, IPX/SPX (Internet Packet Exchange/Sequenced Packet Exchange) ya da AppleTalk gibi daha önce de isimlerinden bahis ettiğimiz protokol yığınları, bu tip bir yapı içinde standart haline gelmiş yığınlardır. Her katmanda bu protokol yığınlarının bir kısmı çalışır.

1.4. TCP/IP

TCP/IP (TransmissionControl Protocol/Internet Protocol), yoğun veri trafiği olan ağlarda gösterdiği performans ve platformdan bağımsız olarak çalışması sayesinde oldukça yaygınlaşmış bir protokoldür. Bugün, İnternet'in bağlı olduğu milyonlarca bilgisayar, TCP/IP protokol yığınını kullanarak iletişim kuruyor. TCP/IP'nin çok basit ve esnek yapısı sayesinde, İnternet'e bağlı olmayan LAN (Local Area Network)'larda da kullanımı gelişmiştir. Daha sonra, İnternet'e açılmak isteyen LAN yöneticileri, TCP/IP'yi kullanarak yaygınlığını pekiştirdiler[20].

Bugün hemen her işletim sistemi, standart olarak TCP/IP protokol yığınını kullanabileceği ayarlarla birlikte geliyor. TCP/IP'nin birbirinden farklı olan işletim sistemlerini de birleştirebilme yeteneği de göz önünde bulundurulduğunda, TCP/IP'nin bugün evrensel bir protokol olduğu sonucuna ulaşmak zor olmaz.

1.4.1. TCP/IP Katmanları

TCP/IP protokol yığını içinde kalan protokollerin tanımlanmasında 4 katmanlı bir referans modelini kullanılıyor. Bu model sayesinde her katmanda yer alan protokollere bakacağız. TCP/IP'ye ait protokolleri ve görevlerini tanımlamak için kullandığımız model, 4 adet katmandan oluşmaktadır. Bu katmanlar şunlardır:

1.4.1.1. Application (Uygulama) Katmanı

Network'e ulaşmak ve network üzerinde iletişim kurmak isteyen tüm yazılımların uygulama katmanında (application layer) yer aldığı kabul edilir. Bu katmanda yer alan temel protokoller, gündelik yaşamda kullandığınız programların nasıl çalıştığını ve bu programların nasıl veri alıp verdiğini belirlemektedir. Bu katmandaki protokoller, kullanıcıların, talep ettiği bilginin, ilk olarak nasıl ele alınacağını belirler[18].

HTTP (HyperText Transfer Protocol), SMTP (Simple Mail Transfer Protocol), FTP (File Transfer Protocol), SNMP (Simple Network Manağement Protocol) gibi protokoller bu katmanda yer alırlar. Bu protokollerden bazıları hakkında bilgiler ve bu katmanda gerçekleşen işlemler ve katmanın içeriği hakkında bilgi verecek olursak:

HTTP (HyperText Transfer Protocol – HiperMetin Aktarım Protokolü): HTTP, İnternet'te bağlandığınız Web sayfalarının kodlarını aktarmak için kullandığımız protokoldür. Örneğin www.turktelekom.com.tr yazdığımızda, ilk olarak bu protokol alt seviyedeki protokollere bu adresin nereden, nasıl isteneceğini ve nasıl aktarılacağını söylemektedir[20].

FTP (File Transfer Protocol – Dosya Aktarım Protokolü): FTP, İnternet'e ait bir servis olarak da düşünülebilir ve bu servis İnternet gibi TCP/IP tabanlı network'lerde dosya aktarmak için kullanılmaktadır. FTP servisinde, örneğin, ftp.intranet.com.tr gibi bir adresten bir dosyanın alınması istediğinde, FTP protokolü çalışmaya başlar. Bu noktada dikkat edilmesi gereken husus, ftp.intranet.com.tr adresinin İnternet'te bulunması ve buna ait isteklerin, bir network kablosuna ham elektrik sinyalleri olarak ulaşıncaya kadar, isimden daha sonra göreceğimiz IP adresi çözümleme işlemine kadar her safhanın TCP/IP'nin tanımladığı ortam ve kurallar içinde yapılmış olmasıdır. Örneğin www.turktelekom.com.tr ya da ftp.intranet.com.tr gibi bir adresin İnternet üzerinde, ulaşılabilecek bir bilgisayarı temsil etme kavramı, TCP/IP'nin DNS (Domain Name System) isimli bir servisi sayesinde olmaktadır[20]. Kısacası, TCP/IP bir network'te isimlerin nasıl verileceğinden, elektrik sinyallerinin nasıl oluşturulacağına kadar her noktada görev yapan protokollere sahiptir. Bu durumdan da anlayabileceğimiz şey, TCP/IP içindeki protokoller ancak birbirlerinin standartlarından ve verileri ele alış biçimlerinden haberdar oldukça işlemlerin sürdüğü gerçeğidir. Kısaca bir protokol yığını, isim vermekten, elektrik sinyallerinin belirlenmesine ve kullanılmasına kadar her noktada birbiriyle uyum içinde olan protokollerle müdahale eder ve network'ü yönetir.

SMTP (Simple Mail Transfer Protocol – Posta Aktarım Protokolü): Microsoft Outlook gibi bir yazılımdan e-posta göndermek istediğinizde, bu protokol tetiklenmiş olur. Protokol,örneğin network@turktelekom.com.tr gibi bir adresten, e-posta gönderileceğini anlar ve e-postaların nasıl gönderileceğinden hangi adrese gönderileceğine kadar her tür işlemin başlamasını ve alt katmanda incelenmesini sağlar[20].

Bu katmanda, daha sonra birkaç bölüm boyunca değineceğimiz, DNS servisleri, Telnet servisi gibi protokoller ve standartlardan oluşan kavramlar da yer alırlar.

1.4.1.2. Transport (İletim) Katmanı

İletim katmanı (transport layer), iki bilgisayar arasında iletişimin kurulmasından ve sürdürülmesinden sorumludur. Örneğin, HTTP protokolü, www.turktelekom.com.tr adresindeki Web sitesinin görüntülenmesini istemişse, bu adrese ulaşılması ve bu adresteki bilgisayarla olan iletişimin sürdürüldüğüne dair onay bilgisi bu katman tarafından sağlanır[20]. Bu katman, TCP/IP protokol yığınının, bel kemiğini oluşturan iki protokolü içerir. Bu protokoller, daha alt katmanlardan gelen verilerin hangi yazılıma (Uygulama katmanında o anda çalışmakta olan yazılımlar) gideceğini belirlenmesini sağlarlar.

TCP (Transmission Control Protocol): Bu protokol verilerin doğru adrese gidip gitmediğini kontrol eder. Bu işlem için bir tür teyit kullanmaktadır. Verilerin gönderildiği noktadaki bilgisayar ya da cihaz, belli aralıklarla, bu katmanda değerlendirilmek üzere, verilerin doğru alındığını belirten onay mesajları gönderir[20]. TCP, ayrıca hem alıcı bilgisayar için, hem de veriyi gönderen bilgisayar için port bilgisini veri paketlerine ekler. Network üzerinde veri aktaran yazılımlar (örneğin bir DNS Server, MS Messenger, MS Outlook, bir LAN'da dosya kopyalarken kullandığımız işletim sistemi programları, vs) hangi yazılımdan veri istediğini belirtmek için port'ları kullanırlar.

Bu katmanda sayısı en fazla 65.536 olan port'lar bulunmaktadır. Örneğin, Internet Explorer'a giden Web sayfalarınızın verileri, 80. port'a gönderilir. Ya da e-posta adresinizden gelen mailleriniz, 25. port'tan geçecektir.

MS Outlook 25. port'u izler, Internet Explorer da 80. port'u kullanır. O halde veriler bir noktadan bir başka noktaya gönderilirken, veri paketlerinde port bilgisi, ulaştırılacak olan bilgisayarın adresi (TCP/IP kurallarına göre tanımlanmış bir adres) ve onay bilgisi yer alır. Bu port'ların asıl sahipleri ise Application katmanında yer alan, protokollerdir. Örneğin FTP protokolü 20 ve 21. port'tan iletişim kurar. HTTP protokolü de (bu protokol Web sayfalarının aktarılmasında kullanılmaktadır) 80. port'u kullanır. Bir bilgisayar bir IP adresi (o bilgisayara bir network'te nasıl ulaşılacağını gösteren adres) ve bir port belirlediğinde buna soket (socket) ismi verilmektedir. Yani "X IP adresindeki bilgisayara, Y port'undan bilgi gönderildiğinde, bu bilgi şu işlem için ele alınacaktır." şeklinde bir önerme ortaya çıkar.

Örneğin, X IP adresinden 80. port'tan bir veri istediğimizde, bu verinin bir Web sayfası yayımlamakta olan bir Web sunucusu tarafından ele alınacağını biliriz. Bu tip tanımlamalar, bir network'te "...şu adresten ve şu port'tan şu tip işlemler yapılır..."

bilgisini ortaya çıkarır. X IP adresindeki Y port'una network üzerinden bir çağrı paketi atarak haberleşmeyi başlatmaya socket (soket) açmak denir. Network'ten birbirlerini bu şekilde bularak çalışarak yazılımlara soket kullanarak çalışan yazımlar denir. Bunlar Windows'ta çalışan yazılımlarsa, bunlara da windows sockets (winsock) yazılımları denir.

Veri haberleşme altyapılarının planlanması sırasında, isimleri temel alarak yapılandırma tekniği, isimlerin değişmesi ile haberleşme altyapısının çökmesi riskini doğurabileceğinden, network'ler üzerinde genelde tüm operasyonlar değişmeyen sabit eşsiz (unique) sayılar kullanılarak yapılandırılır. Bu sayede bu sayıların tanımladığı servislere isimleri sonradan vermek, bu isimlerin istendiğinde kolayca değiştirebilmesine imkân tanır.

TCP'nin adındaki kontrol lafından da anlayabileceğimiz gibi bu protokol iki bilgisayar arasındaki bilgilerin doğru gidip gelmediğini kontrol eder, eğer gelmemişse bunu karşıdan tekrar istemektedir, eğer geldi ise bunu "Alınmıştır" şeklinde onaylar.

UDP (User Datağram Protocol): UDP protokolü, TCP'ye göre çok daha hızlı veri aktarılmasını sağlamaktadır. TCP'den önemli farkı, yapılacak her haberleşme paketini alındı, gönderildi seklinde, kontrol verilerini karşılıklı kontrol etmeden çalışmasıdır. Bu da karşılıklı veri değiş-tokuşunun (haberleşmenin) daha hızlı olmasını sağlar, ama kontrol olmadığı için, veri kaybı riski doğurur. Arama (query) yapan programlar genelde performans için bu protokolü kullanırlar (örneğin DNS ve WINS (Windows Internet Name Service)). Bu yüzden TCP ile network üzerinden birbirini bularak haberleşen uygulamalara connection oriented (bağlantı yönelimli) denir. UDP kullanarak çalışanlara da connectionless (bağlantısız) denir[17].

UDP, kontrol adına hiç bir şey yapmamaktadır. Bu özelliği ile TCP den daha hızlı çalışır, ancak aktarılan (transfer edilen) verinin doğruluğu garantilenemez. Böyle uygulamalarda, verinin karşıya doğru gönderildiğinin kontrolünü yapmak, uygulamayı programlayan, yazılımcının görevi haline gelir ve programlama hataları, haberleşme sorunları doğurabilir[17].

1.4.1.3. İnternet Katmanı

İnternet katmanı, TCP/IP protokol yığını içinde adresleme, verilerin paketlenmesi ve veri paketlerinin yönlendirilmesi işlemlerinden sorumludur. Bu katmanda ki protokoller şunlardır:

IP (Internet Protocol – İnternet Protokolü): Fiziksel olan bilgisayarların kavramsal bir adres almalarını sağlar[18]. Böylece herhangi bir bilgisayara ulaşılması gerektiğinde, network üzerinde bir adres atanmış olur.

ARP (Address Resolution Protocol – Adres Çözümleme Protokolü): Bir bilgisayara herhangi bir IP numarası verilmiş olabilir. Fakat bu bilgisayara network üzerinde verilerin taşındığı elektrik sinyallerinin ulaşması için sabit noktalara ihtiyaç vardır[18]. Bilgisayarlarda MAC (Media Access Control) adresi denilen ve her bilgisayarın network adaptörü üzerinde bulunan sabit bir numara vardır. Bu numara sayesinde fiziksel olarak, bilgisayarların ürettiği bilgiler birbirlerine ulaşmaktadırlar. Bu noktada IP adresi ile MAC adresi arasındaki ilişkiyi açıklayarak, ne tür görevleri olduğunu da göreceğiz. MAC adresleri, bir bilgisayarın üzerindeki bir network adaptör kartının diğer bilgisayar üzerindeki network adaptör kartına veri gönderirken kullandığı bir adrestir. Örneğin A bilgisayarı, binlerce bilgisayarın bulunduğu bir network'te bir başka bilgisayara ulaşacaksa, ham veri paketlerinin başına ulaşılacak makinenin MAC adresini ekler. Bu sayede veri paketleri karşı taraftaki network kartı tarafından ona ulaştığında, ele alınır. O halde, bu noktada IP adresi ile olan bağlantıyı sorgulayalım.

IP adresleri, bir makineye kullanıcı ya da onun üzerinde çalışan programlardan biri tarafından verilmiş olan sanal bir adrestir. IP adresleri, MAC adreslerinden farklı olarak, bilgisayarın parçalarından birinde değiştirilemeyecek şekilde kodlanmış bir bilgi değildir. IP adresleri, işletim sistemi üzerinden elle ayarlanabilir. Bir bilgisayar birden çok IP adresi de alabilir. Bu noktada amaç şudur: Örneğin X kullanıcısının kullandığı bir bilgisayar üzerinde birden çok işlem gerçekleşiyorsa, o takdirde o bilgisayara her görevde özel olarak kullanılan bir IP tahsis edilebilir. 100 adet bilgisayarın olduğu bir network'te bazı bilgisayarların birden çok IP ile ulaşılabilir şekilde ayarlanması sonucunda, o network'te 100'den çok IP adresi olabilir. Bu noktada şuna dikkatinizi çekmek gerek: Bir bilgisayarın IP adresi ne olursa olsun ya da kaç tane olursa olsun, MAC adresi sabittir ve değiştirilemez. Zira bu adres network kartının içinde daha öncede değiştirilemeyecek şekilde (üretildiği esnada) kaydedilmiştir. Ve bilgisayarların üzerindeki network adaptörleri, birbirleriyle iletişim kurarken MAC adresleri ile iletişim kurarlar[18].

Bir MAC adresi ile ulaşılan bir bilgisayarda birden çok IP adresi olabilir. Ve aslında network üzerinde, şu MAC adresli bilgisayarda şu IP adres(ler)i var gibi tanımlamalar yapılmış olur. ARP protokolü, bilgisayarların içinde yer alan network adaptörlerinin, kendi

aralarında konuşurken MAC adreslerini kullanmalarını ve bu iletişim hangi kurallarla yapılacağını belirleyen bir protokoldür.

ICMP (Internet Control Messağe Protocol – İnternet Kontrol Mesajı Protokolü): ICMP protokolü, verilerin taşındığı sırada, oluşan problemler yüzünden veri ulaştırılamadığı hallerde, hata durumunun oluşturulmasından sorumludur[18]. Herhangi bir veri paketinin yerine ulaşmaması durumunda bu protokol verinin yerine ulaşmadığını bildiren bir mesajı üst katmana iletir. Bu sayede, networkte kayıp olan ya da bozulan veri paketlerinin tekrar iletilmesi için mekanizmalar tetiklenmiş olur.

IGMP (Internet Group Manağement Protocol – İnternet Grup Yönetim Protokolü): IGMP protokolü, multicasting işleminin yürütülmesinden sorumludur[18]. Bu protokol sayesinde, multicast gruplarının kim olduğu ve ulaşılabilirlik durumu, router cihazlarına iletilir.

1.4.1.4. Network Arabirim Katmanı (Network Interface Layer)

Network arabirim katmanı, TCP/IP katmanlarının en altında yer alan katmanıdır. Verilerin, network'ü oluşturan, kablo ya da radyo sinyalleri gibi, veri aktarım ortamına yerleştirilmesini sağlar. Veriler network kablosu ya da benzer bir veri aktarım ortamına aktarılabilecek duruma geldiğinde bu katmana iletilirler. Bu katmanda, yazılım olarak yer alan protokoller yer almaz.

1.5. Ağ Bağlantı Cihazları

Ağlarda segmentler (bölümler) arasında veri iletimini sağlayan birtakım cihazlar vardır. Bu cihazlardan bir kısmı yerel alan ağlarında, bir kısmı geniş alan ağlarında kullanılmaktadır. Bazı cihazlar hem yerel alan ağlarında hem de geniş alan ağlarında kullanılmaktadır. Bilgisayar ağlarında genel olarak kullanılan cihazlar şunlardır: Hub, switch, repeater, bridge, router.

1.5.1. Hub (Göbek)

Hub'lar, yıldız (star) topoloji ağlarda, merkezi bağlantı üniteleridir. Hub, kendisine bağlanılan tüm node'ların birbirleri ile iletişim kurmasını sağlar. Node; bir network

ekipmanı (hub veya switch gibi) ile haberleşebilen sunucu, yazıcı, faks makinası vb. aygıtlardır. Hub'a bağlanılan her ekipmanın kendi güç kaynağı olduğu gibi, hub'ında kendi güç kaynağı vardır. Hub üzerinde bulunan durum ışıkları, ağ durumunun izlenmesini ve arıza tespit işlemlerini kolaylaştırır. _kiden fazla hub birbirine bağlanabilir fakat Ethernet standartlarında bazı sınırlar vardır. Hub-Hub bağlantıları yerine switchlerden hub'lara gidilebilir ve bu durum ağ performansını arttırır. 10 Mbps veya 100 Mbps ağlar için hub'lar bulunmaktadır. Üzerinde genellikle 5 ile 32 bilgisayarın bağlanabileceği port bulunur. Ağ üzerindeki bilgisayarlar, UTP türü kablo kullanarak huba bağlanırlar. Birden çok hub birbirine bağlanarak (en fazla üç adet) ağ daha da genişletilebilir.

Hub'ın görevini özetleyecek olursak; kendisine ulasan sinyalleri alıp, yine kendisine bağlı olan ağ ekipmanlarına dağıtır. Hub, bu işlem sırasında bir tekrarlayıcı görevi görür ve sinyali güçlendirir[19].

1.5.2. Switch (Anahtar)

Switchler bir ağı daha küçük, denetlenebilmesi kolay alt ağlara böler. Böylece ağ hızı artar. Switchler daha kompleks ve daha verimli hub' lardır. Büyük bir ağı segmentlere (parçalara) bölerek, ağ performansını arttırır. Herhangi bir node'tan gelen verinin, tüm ağa dağıtılması yerine, istenilen node'a dağıtılmasını sağlar. Ağ durumunu izler, veriyi gönderip, iletim işleminin yapılıp yapılmadığını test eder. Bu özelliğe; "store and forward" (depola ve ilet) denir[19].

1.5.3. Repeater (Yineleyici)

İki ya da daha fazla bilgisayar ağını birbirine bağlamak için kullanılan en kolay yol; "Repeater" kullanmaktır. Bu aygıtlar ağın uzak yerleşimlere erişmesini sağlarlar. Bu aygıtların işlevi, ağ içindeki sinyalleri kuvvetlendirip diğer ağa taşımaktır. Örneğin, iki segment arasındaki uzaklık kalın koaks kablolarda 500 metre ve ince koakslarda 185 metredir. Daha fazla uzaklığa kablolama gerekiyor ise bu limitlerde zayıflayan sinyallerin güçlendirilmesi lazımdır. Yineleyiciler sayesinde daha uzak ağlar birbirine bağlanabilir. Genellikle ince ve kalın koaks kablolarda kullanılırlar. UTP tipi kablolarda zaten hub'lar birer yineleyici görevini görmektedir. Token Ring sistemlerinde ağa bağlı her is istasyonu

kendisine gelen paketi güçlendirdiği için yineleyicilere gerek duyulmaz. Ethernet ağlarında en fazla üç adet repeater kullanılabilir. Repeater'lar, kurulumlarının kolay olması, maliyetlerinin az olması ve az bakım gerektirmeleri nedeniyle bilgisayar ağlarında sıkça kullanılırlar[19].

1.5.4. Bridge (Köprü)

Bridgeler; OSI modelinin veri bağlantı katmanında çalışmaktadırlar. Birbirlerinden bağımsız iki ağın bağlanması için kullanılırlar. _ki ağı birleştirirler ve bilgi paketlerinin geçişini sağlarlar. Bridge'ler, üst düzey protokoller arasındaki uyumluluğu göz önünde bulundurmadan yönlendirme yaparlar. Bridgeler, gelen her çerçeveyi aktarmadan okur, hata denetimi yapar ve saklar. Çerçevenin nereden geldiğini ve nereye gönderileceğini MAC adreslerinden yararlanarak anlarlar. Bridgelerin faydaları söyle sıralanabilir: Yerel alan ağlarının genişlemesini sağlar. Bir yerel alan ağını bridgeler ile parçalara (segmentlere) bölmek performansı arttırır. Bridgeler ile birleştirilmiş iki ağ, farklı MAC alt katmanı protokolü kullanabilir[19].

1.5.5. Router (Yönlendirici)

Büyük ve değişik protokollere sahip bilgisayar ağlarını birleştirirler. Router, OSI modelinin ağ katmanında çalışır. Router'lar, bir ağ üzerindeki tüm bilgisayarların adreslerini bilir ve buna göre kendilerine gelen paketi en uygun şekilde hedefe yollarlar. Router'lar, genellikle dinamik yönlendirmeyi kullanırlar[15]. Bunun anlamı, kendisine gelen bir paketin tüm ağ taranarak, en güvenli ve hızlı yolun denenmesidir. Verinin içeriğini incelerler ve iletilmesi gerekmiyorsa iletmezler. Eğer herhangi bir sorun çıkarsa, alternatif bir yol arayarak mutlaka paketi hedefine ulaştırmaya çalışırlar. Bridge'lerden farklı olarak router'lar, sadece alt ağ adreslerini bilirler, her paket ya da çerçevedeki adres bilgilerini okurlar, yolu belirleyerek veriyi paketler ve gönderirler. Yönlendiriciler; ağa bağlı özel bir araç veya ağa bağlı bir bilgisayar olabilirler.

1.6. Kablosuz Yerel Alan Ağları

Kablosuz Yerel Alan Ağları (Wireless Local Area Networks, WLANs), iki yönlü geniş bant veri iletişimi sağlayan, iletim ortamı olarak kablo yerine radyo frekansı veya kızılötesi ışınları kullanan ve bina veya kampüs gibi sınırlı bir alanda çalışan iletişim ağlarıdır[21].

Kurulum kolaylığı ve hareket serbestliği gibi önemli avantajlar sağlayan WLAN sistemleri kablolu ağların yerini alabilmekte hatta bu ağlara göre daha fazla fonksiyonlar içerebilmektedir. Kablosuz Yerel Alan Ağları Avrupa düzenlemelerinde Telsiz Yerel Alan Ağları, Radio Local Area Networks, Radio LAN, RLAN olarak adlandırılmasına karşın başta ABD olmak üzere birçok ülkede Wi-Fi (Wireless Fidelity – Kablosuz Bağlılık), Wireless Local Area Networks, Wireless LAN, WLAN **(**Kablosuz yerel alan ağları) olarak adlandırılmaktadır[21].

WLAN sistemleri iş adamları, yöneticiler, çalışanlar, küçük işletmeler, orta ölçekli işletmeler ve bireysel kullanıcılar gibi büyük bir kesime internet ve üyesi oldukları kurumsal ağa (Intranet) mobil olarak bağlanma imkanı sağlamaktadır. Ayrıca, WLAN sistemleri kullanıcılara mekandan bağımsız olarak kolay bir kablosuz ağ kurulumu ve geniş bant veri iletimi imkanı sunmaktadır [1, 2]. Kablolu LAN'ların tüm özelliklerine sahip olan WLAN sistemleri bu ağların devamı ya da alternatifi olarak kullanılmaktadırlar.

1.6.1. Mimari

802.11 ağların (WLAN) mimarisi temel olarak birbirini kısmen kaplayabilen hücrelerden oluşur. Temel Servis Kümesi (Basic Service Set - BSS) tek bir hücrenin kapsama alanını temsil eder. Bir BSS'in dışında kalan bir istasyon (STA) bu BSS içinde kalan diğer istasyonlar ile haberleşemez.

802.11 standartları iki modda çalışmaktadır. Bunlardan ilki BSS olarak da bilinen altyapı modu diğeri ise Bağımsız BSS (Independent BSS- IBSS) olarak bilinen Bağımsız (Ad hoc) moddur.

1.6.1.1. Bağımsız (Uçtan Uca) Model (Ad Hoc Mod)

En basit WLAN yapısı Bağımsız (ad hoc veya peer-to-peer) WLAN'dir. Bu WLAN NIC ile donanmış bir grup bilgisayarın kurdukları ağın ismidir. Bu tip konfigürasyona sahip bir ağda erişim noktasına ihtiyaç duyulmaz ve noktadan noktaya haberleşmeyi sağlamak amacıyla yerel ağ aynı radyo frekans kanalında çalışır. Birbirinden farklı ağlar ancak kablosuz adaptörler birbiriyle haberleşebilecekleri mesafedeyse oluşturulabilir.

Bu yapıda, her kullanıcı ağdaki bir diğeri ile direkt iletişim kurar. Bu mod, birbirleri ile iletişim mesafesinde olan kullanıcılar için tasarlanmıştır. Eğer bir kullanıcı bu tanımlanmış mesafeden dışarıya çıkarak iletişim kurmak isterse, aradaki bir kullanıcı, ağ geçidi ve yönlendirici olarak görev yapmak zorundadır. Şekil 1'de bağımsız WLAN mimarisinde ağ elemanlarının yerleşimi görülmektedir.

Şekil 1. Bağımsız (Ad Hoc) WLAN Mimarisi[21].

1.6.1.2. Altyapı Modeli (Infrastructure Mode)

Infrastructure WLAN kablosuz istasyonlar (bilgisayarlar ve/veya iş istasyonları) ve erişim noktalarından (AP) oluşur. Erişim noktaları bir dağıtım sistemine (Ethernet gibi) sahipse birden çok radyo hücreleri birbirleriyle roaming yaparak haberleşebilirler. Erişim noktaları sadece kendi kablosuz ağı ile kablolu ağları haberleştirmekle kalmaz aynı zamanda komşusu olan diğer kablosuz ağlar ile de haberleşmeyi sağlar.

Şekil 2. Altyapı Moda WLAN Mimarisi[21].

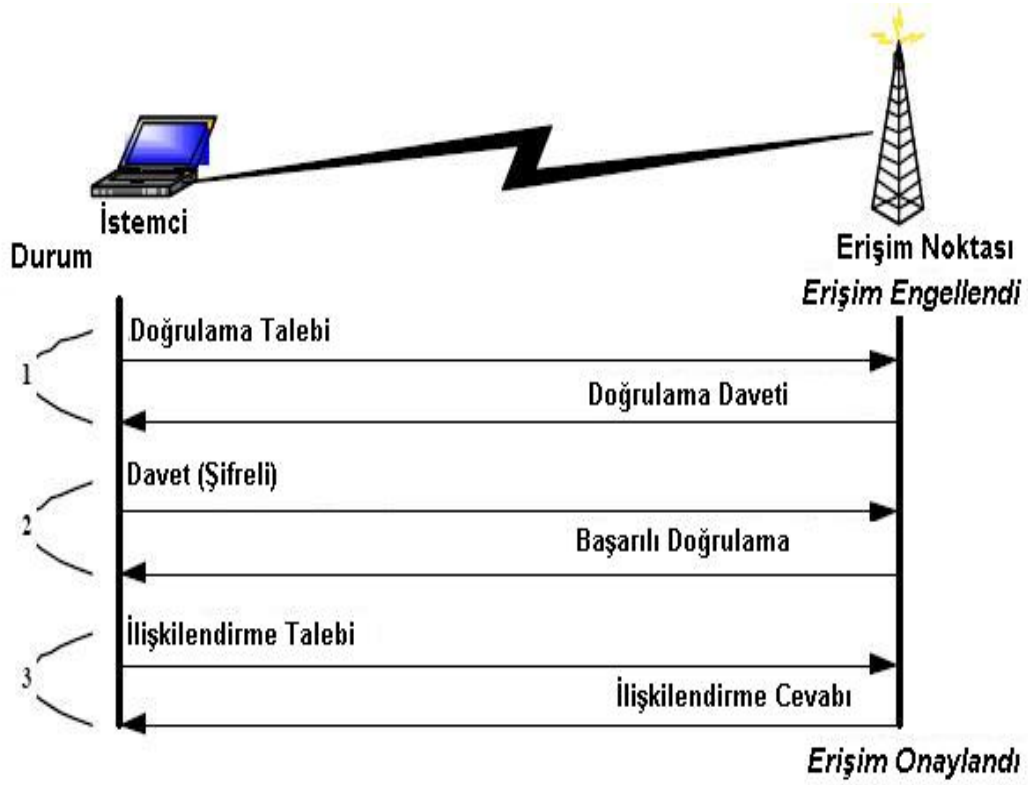
Şekil 2'te tek AP (Access Point) içeren ve altyapı modunda çalışan bir ağın genel yapısı görülebilir. Bir AP tarafından koordine edilen alana BBS (Basic Service Set) ismi verilmektedir. Bunun anlamı 'bir tek koordine merkezi tarafından idare edilen bir grup istasyondur'. Geniş ağlarda AP'ler de birbirine kablolu ağlar yardımı ile bağlanmaktadır. Kablolu ağlarda bir ağı tanımlamak için Ağ Adresi (Network Address) kullanılmaktadır. Kablosuz ağlarda ise ağı tanımlamak için ise SSID (Service Set Identifier) kullanılmaktadır. Kullanımı ise şu şekildedir: Bilgisayarda yüklü yazılım yardımı ile bağlanılabilecek SSID numaraları belirlenir ve bunlardan biri seçilerek ilgili ağa bağlantı yapılır. Tabii ki bilgisayarların bu SSID numaralarına erişebilmeleri için AP'lerin bu numaraları çeşitli aralıklarla yaymaları (broadcast) gerekmektedir. Aynı alan içerisinde farklı komünikasyon kanallarını kullanan (Örneğin, frekans bölümlemeli çoğullama yöntemi) ağlar mevcut olabilmektedir.

Altyapı modunda her istasyon bağlantı isteklerini erişim noktası (AP) olarak bilinen merkez istasyona yollar. AP'ler bildiğimiz kablolu ağ anahtarları gibi çalışır ve iletişimi kablolu veya diğer bir kablosuz ağa yönlendirir. AP'ler ve istasyonlar arasında veri iletişimi ancak iletişim sağlandıktan sonra başlar. Bir ortamda kablosuz iletişim başlamadan önce hizmet almak isteyen istemci (client) ile AP arasında bir ilişki (association) bulunmalıdır. Bunun ile ilgili olarak üç yöntem bulunmaktadır:

a) Doğrulanmamış ve ilişkilendirilmemiş: Kullanıcının ağ ile doğrulama ve ilişkilendirme işlemlerini gerçekleştirmediği durumdur.

b) Doğrulanmış ve ilişkilendirilmemiş: Kullanıcının ağ ile doğrulama işlemi gerçekleştirdiği fakat henüz ilişkilendirme işlemini gerçekleştirmediği durumdur.

c) Doğrulanmış ve ilişkilendirilmiş: Kullanıcının ağ ile doğrulama ve ilişkilendirme işlemlerini tamamlandığı durumdur.

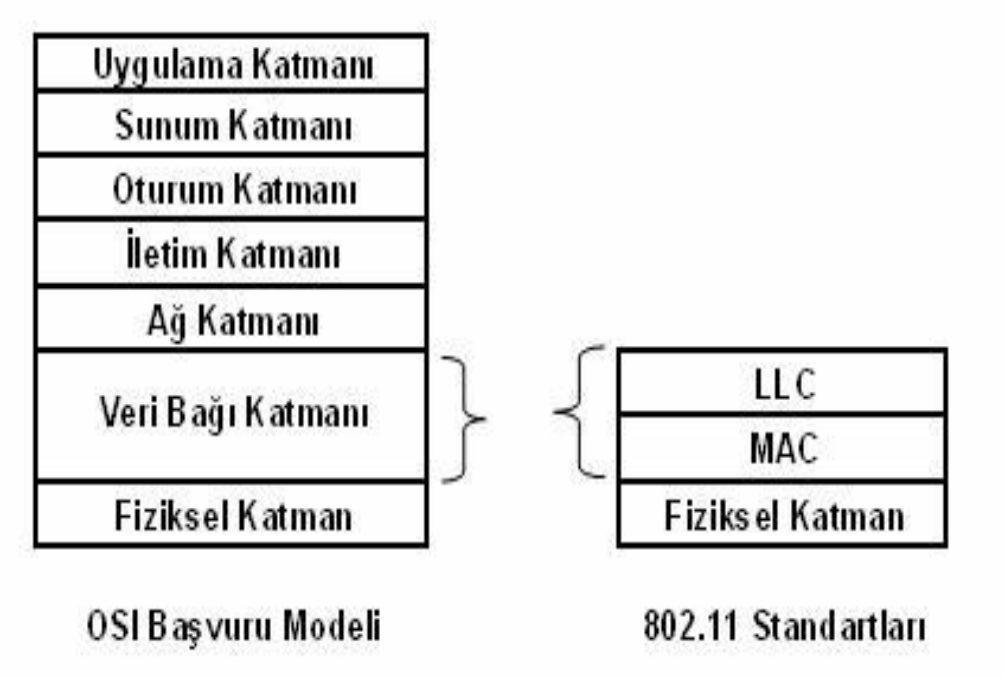


Şekil 3. Doğrulama ve İlişkilendirme Durumları[21].

Genel olarak kullanılan yöntem 'Doğrulanmamış ve ilişkilendirilmemiş' yöntemidir. Yani AP ile iletişime geçmek isteyen bir bilgisayarın, iletişime geçmeden önce herhangi bir ön protokol ile ilişki kurmaya ve bilgiyi kontrol edip, doğrulamaya gereksinimi yoktur.

1.7. Kablosuz Bilgisayar Ağlarında Kullanılan Standartlar

OSI başvuru modeline göre üst katman protokolleri, ağ mimarisinden bağımsızdır ve LAN, MAN ve WAN‘ lar da uygulanabilir. Bu nedenle, bir yerel alan ağ protokolleri ilk iki katmanla ilgilidir[3].



Şekil 4. OSI başvuru modeline göre IEEE 802.11 katmanları[21].

IEEE 802 standardının ilk katmanı olan Fiziksel Katman, OSI Başvuru Modelinin ilk katmanı olan Fiziksel katmana denk gelmektedir ve aynı fonksiyonları içermektedir. Bunların yanında, gönderim ortamı ve mimari ile ilgili tanımlamaları da içermektedir. Fiziksel katmanın üzerinde, LAN kullanıcılarına servis sağlamayla ilgili işlevleri içeren katman vardır. Bu katman, OSI Başvuru Modelindeki Veri Bağı (Data-Link) katmanına denk gelmektedir, fakat IEEE 802 Başvuru Modelinde Mantıksal Bağ Kontrol (Logical Link Control - LLC) Katmanı ve Ortama Erişim Kontrol (Medium Access Control - MAC) katmanı olmak üzere 2 ayrı katmana ayrılmıştır (Sekil4).

Protokol Adı	Ayrıntı
802.1	Ağlar ve sistem yönetimi hakkında genel tanımlamalar
802.2	LLC alt katmanını tanımlar
802.3	Ethernet – CSMA/CD yol erişim yönetimi
802.3u	100Base-T
802.3z	Gigabit Ethernet
802.4	Token Bus tanımlaması
802.5	Token Ring Tanımlaması
802.11	Kablosuz LAN
802.13	100VG-anyLAN
802.15.1	2,4 GHz ISM bandında Bluetooth'a dayanarak kablosuz kişisel ağ (PAN)
802.16	Wi-max Geniş alan kablosuz erişim

Tablo 1. IEEE yerel alan ağı standartları[19]

Kablosuz ağlar ile Ethernet standardı arasında OSI başvuru modeline göre fiziksel katman ve veri bağı katmanı düzeylerinde farklılıklar görülmektedir (Sekil-3.8). Kablosuz ağların çalıştığı fiziksel ortam kablo içermediğinden fiziksel katman kablosuz haberleşme standartlarını ve modülasyon tekniklerini içermektedir. Veri bağı katmanı ise yine OSI başvuru modelinde olduğu gibi iki alt katmana ayrılmıştır: MAC (Media Access Kontrol-Ortam Erişim Kontrolü) ve LLC (Logical Link Conrol- Mantıksal Bağlantı Kontrolü). MAC alt katmanı iletişim kanalının nasıl ayrılacağını belirlerken, LLC alt katmanının

görevi farklı protokoller arasındaki değişiklikleri ağ katmanına belli etmemektir. Kablosuz ağları üç ana sınıfta değerlendirmek mümkündür:

1. Sistemler arası bağlantılar ye da kişisel alan ağları (WPAN)
2. Kablosuz yerel alan ağları (Wireless LAN)
3. Kablosuz geniş alan ağları (Wireless WAN)

Bir bilgisayara çeşitli çevre birimlerinin bağlanmasıyla meydana gelen kısa mesafeli kablosuz ağlar, sistemler arası bağlantı olarak adlandırılmaktadır [25]. Kablosuz yerel alan ağları ise her bilgisayarın diğer bilgisayarlarla haberleşebileceği bir kablosuz modemi ya da anten sistemi bulunmaktadır. Bu tür bağlantılar ofis uygulamalarında, özellikle taşınabilen bilgisayarların kullanıldığı ortamlarda Ethernet'in yerini almaktadır. Kablosuz LAN uygulamalarında kullanılan IEEE 802.11 ve HiperLan standartları gün geçtikçe yaygınlaşmaktadır. Kablosuz geniş alan ağları, daha geniş alanlara yayın yapabilen, kapsama alanı kilometreler ile ifade edilen, yüksek oranlı veri gönderme hızına sahip LMDS (Local Multipoint Distribution Service)ve WATM (Wireless Asynchronous Transmission Mode) standartlarını içermektedir[4].

1.8. Kablosuz Yerel Alan Ağı Sistemlerinin Avantajları

Kablosuz LAN'ın en açık avantajı; kullanıcılara, bulundukları yerde gerçek zamanlı bilgi girişi sağlamasıdır. Ayrıca; hareketlilik üretkenliği artırır ve kablolu ağlarda mümkün olmayan hizmet olanakları sağlar.

Şirketler, ağ kurulum ve yönetim masraflarını, kablosuz LAN kullanarak önemli ölçüde azaltmışlardır. WLAN sistemleri; kablosuz olmanın avantajlarını kullanarak, kablo çekmenin zor, pahalı veya imkansız olduğu yerlerde kolay ve düşük maliyetli iletişim imkanı sağlamaktadır.

Bina içi kullanımda WLAN sistemlerinin kurulumu, oldukça hızlı ve kolaydır. Çünkü, duvar ve tavanlardan kablo çekme zorunluluğu bulunmamaktadır. Sadece AP'nin monte edilmesi, sistemi kurmak için yeterlidir. Yine kablo döşenmesine izin verilmeyen tarihi yapılarda, WLAN sistemi uygun bir çözüm olmaktadır.

WLAN sisteminde bilgisayarların montaj yerlerini belirlemeye ve kablolamaya ihtiyaç duyulmaz. Çünkü, bilgisayarların kapsama alanı içinde olması yeterlidir.

Kullanıcı sayısının ve yerinin (konumunun) değişken olduğu ortamlar için WLAN sistemleri oldukça elverişlidir. Ayrıca, sisteme yeni kullanıcıların katılması durumunda da

ilave malzeme ve işçilik harcaması gerekmemektedir. Kablosuz erişim özelliğine sahip bir cihaz, sisteme kolaylıkla dahil edilebilir veya çıkarılabilir[5].

Yukarıda da açıklandığı gibi, kablosuz LAN'lar kullanılarak birçok avantaj elde edilebilir. Bu avantajlar bina içi ve binalar arası olmak üzere sınıflara ayrılarak, yukarıda değinilen avantajlar maddeler halinde yazılacak olursa:

Bina içinde:

• Hareket özgürlüğü sağlanır.

• Kurulumu için kablolama yatırımı yapılmayacağından, kablolama masrafı olmaz.

• Kablo çekmenin zor, pahalı veya imkansız olduğu yerlerde kolay ve düşük maliyetli iletişim imkanı sağlanır.

• Sadece AP'nin monte edilmesi sistemi kurmak için yeterli olur.

• WLAN sisteminde bilgisayarların montaj yerlerini belirlemeye ve kablolamaya ihtiyaç duyulmaz.

• Kullanıcı sayısının ve yerinin (konumunun) değişken olduğu ortamlar için, WLAN sistemleri oldukça elverişlidir. Ayrıca, sisteme yeni kullanıcıların katılması durumunda da ilave malzeme ve işçilik harcaması gerekmemektedir.

• Kablosuz ağlar, kurulacak sisteme göre değişmekle birlikte, genellikle kablolu ağlara göre daha düşük maliyetlidir. Çünkü, kablo maliyeti ve kablolama işçiliği ücreti yoktur.

• Ağ idaresi açısından, bakım maliyetlerinin düşüklüğü ve ağdaki bilgisayarların kolayca yer değiştirme imkanına sahip olması, isletme ve bakım masraflarını en az düzeye indirgenir.

• Oteller, tatil köyleri, kütüphaneler, konferans salonları, fuarlar, üniversiteler, kampüsler, havaalanları gibi ortamlarda her yerden mobil internet erişimi sağlanır.

• Roaming (yer değiştirebilme) özelliği ile daha fazla kapsama alanına sahip olur.

• 128 bit şifreleme ile maksimum bilgi güvenliği sağlanır.

Binalar arasında:

• 11 Mbps hızında yüksek hızlı bağlantılarla, karasal bağlantılara alternatif olmaktadır.

• Sabit iletişim / bakım giderleri, en az düzeye indirgenir.

• 128 bit şifreleme ile maksimum kurumsal iletişim güvenliği sağlar.

• Dağınık yapıya sahip isletmeler için, binalar arası kablosuz bağlantı gerçekleştirilir.

1.9. Kablosuz Yerel Alan Ağı Sistemlerinin Dezavantajları

Yukarıda da değinildiği üzere, WLAN sistemlerinin birçok avantajı vardır. Ancak bu avantajlarının yanı sıra bazı dezavantajları da bulunmaktadır. Standartlaşma, ürün seçenekleri, maliyet, frekans tahsisi gibi sorunlar başlangıçta fazla olmasına rağmen, ilerleyen zamanlarda bu sorunlar azalmaya, çözülmeye başlanmıştır. Ancak bazı sorunların giderilmesi için yapılan çalışmalar hala devam etmektedir.

WLAN'ların dezavantajlarından bir tanesi "Güvenliktir". izinsiz kullanımları ve saldırıları önlemek amacıyla güvenlik sistemleri kullanılmaktadır. Kablosuz sistemlerde, kablolu sistemlere göre, güvenlik konusunda daha hassas davranılmalıdır. Çünkü kablosuz sistemleri dinlemek daha kolaydır. Kablosuz sistemler radyo frekansını kullanarak hava yoluyla iletişimi sağlarlar ve radyo frekansının dinlenmesini önlemek imkansızdır. Genelde WLAN sistemleri için, WEP (Wired Equivalent Privacy) güvenlik mekanizması kullanılmaktadır. WEP güvenlik sisteminde; kullanıcı ve erişim noktası tarafından statik 64 bit'lik veya 128 bit'lik kodlama yapılarak, iletilen verinin güvenliği sağlanmaktadır. Bu sistemde, kullanıcının kim olduğuna bakılmaksızın, kablosuz cihazdaki kart sisteme tanıtılmaktadır. Bu durumda; istenmeyen kişiler, çeşitli yöntemlerle kendi kartlarını sisteme tanıtarak giriş yapabilmektedirler. WEP sisteminin eksiklerini gidermek üzere, Wi-Fi Protected Access (WPA) güvenlik sistemi geliştirilmiştir. WPA'da veri miktarı veya zamana bağlı olarak değişen güvenlik anahtarı kullanılmaktadır.

WLAN'ın bir diğer dezavantajı ise "Enterferanstır" (girisim). WLAN sistemleri genellikle ISM bandını kullandıklarından enterferansa açıktır. Özel frekans tahsisli sistemlerin, enterferansa maruz kalma olasılığı daha düşüktür. WLAN sistemlerinin, bulundukları bölgeye bağlı olarak, diğer sistemler tarafından enterferansa maruz kalma olasılıkları yüksektir. Ayrıca WLAN sistemlerinin, birbirlerini enterfere etme olasılıkları da vardır. Bu durum, özellikle RF'in kapsanmak istenilen alanın sınırları dışına taştığı durumlarda veya kamuya açık alanlarda olmaktadır.

WLAN'ın bir diğer dezavantajı ise iletişim mesafesinin kısa olması.. WLAN sistemlerinin bir diğer dezavantajıdır. Kullanılan frekans bandı ve standartların müsaade ettiği kısıtlı çıkış gücü nedeniyle, WLAN sistemlerinin mesafesi 100 m civarındadır. Açık

alanlarda bu mesafe, 300 m civarına kadar artmaktadır. Ayrıca; kazançlı anten kullanılarak, bu mesafeyi çok daha fazla artırmak mümkündür. Benzer şekilde duvar ve mobilya gibi fiziksel engellerin fazla olması durumunda bu mesafe 10 metreye kadar düşebilmektedir.

WLAN sistemlerinde kullanıcıya büyük avantaj sağlayan "Mobil olma özelliği", teknik açıdan önemli sorunlar yaratmaktadır. Bu da WLAN sistemleri için bir dezavantaj getirmektedir. Mesela, taşınabilir bilgisayarların batarya ömrü birkaç saat ile sınırlıdır. Ayrıca bağlantı sorunları da yaşanmaktadır. Çünkü; kablosuz bağlantı için, mobil cihazda uygun ayarların yapılması gerekmektedir.

1.10. 802.11 Yerel Alan Ağlarında Güvenlik

802.11 ağlarda kablosuz iletişimin güvenliğinin gelişimi aşağıdaki yöntemlerin kronolojik olarak geliştirilmesi ile sağlanmıştır.

- WEP (Wired Equivalent Privacy)
- WPA (Wi-Fi Protected Access)
- WPA2 (IEEE 802.11i)

Kronolojik sıra ile ilk olarak WEP algoritması geliştirilmiştir. WEP algoritmasının kullanıma başlaması ile birlikte önemli güvenlik açıkları tespit edilmiştir. Bu açıkları gidermek için iki aşamalı bir çözüm başlatılmıştır. Uzun vadeli olan çözüm IEEE tarafından oluşturulan bir çalışma grubu 'TGi' tarafından tam olarak güvenli bir protokolün oluşturulması şeklinde kararın verilmesidir. Bu grup çalışmalarına başlamıştır fakat sektörün WEP algoritmasındaki güvenlik zaaflarından etkilenmemesi ve biraz da olsa güvenlik önlemlerinin arttırılması için WEP algoritmasının eksik yönlerinin geçici yöntemlerle giderilmesi için Wi-Fi grubu ve IEEE tarafından WPA geliştirilmiş ve sektör için geçici bir çözüm üretilmiştir[8].

802.11'in ilk güvenlik tanımlaması; "Wired Equivalent Privacy" (Kabloluyla Eşdeğer Güvenlik) protokolüydü. Tamamlanmasından sonra, WEP için ciddi güvenlik zayıflıkları belirlendi ve güvenliğin kritik olduğu yerlerde hemen hemen hiç kullanılmamaya başlandı. Bunun üzerine, 802. 11 Görev Güçleri (Task Force) 802. 11 standardına uygun, daha sağlam güvenlik tanımlamaları üretmek için harekete geçti. 802. 11 standardının gelecek nesil güvenlik standardını tanımlaması için, 802. 11 Görev Güçleri (Task Force) 802. 11 Görev Grubu-i (Task Group i- TGi) adını almıştır ve yeni bir standart geliştirmiştir. Yeni

standart, 802. 11i olarak da bilinen, “Robust Secure Network” (RSN- Sağlam Güvenli Ağ) olarak adlandırılmıştır[9].

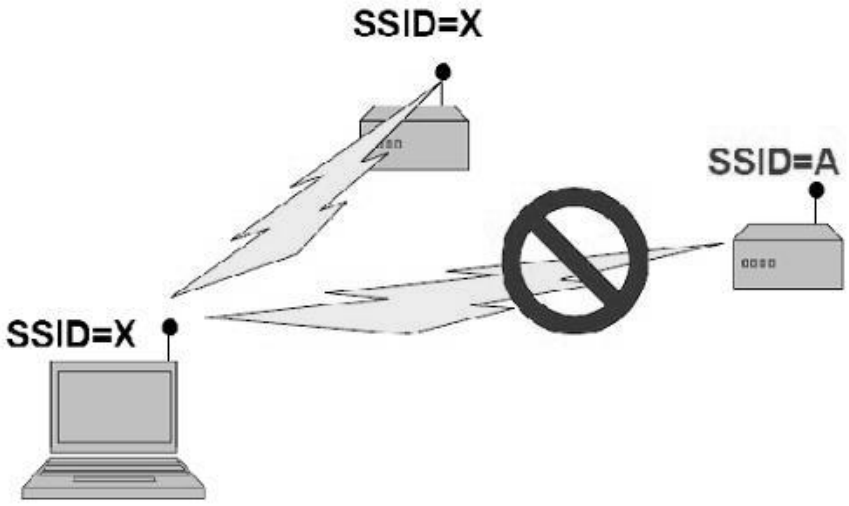
RSN (Robust Security) Network, temel WEP standardının sayısal gereksinimini arttırmıştır. Bu gereksinim; daha kompleks bir şifreleme algoritması kullanılmasından ve otomatik anahtar yönetiminden gelmektedir ve yeni bir donanıma ihtiyaç duyulmaktadır. Kablosuz ağlarda var olan donanımların tamamı değiştirilmeden, ağların daha güvenli hale gelmesini sağlayabilen bir çözüme gereksinim duyulmaktaydı[18].

1.10.1.Geleneksel WLAN Güvenliği

1.10.1.1. Servis Kümesi Belirleyicisi (Service Set Identifier-SSID)

802.11 standardı SSID’yi kullanıcı belirli bir kablosuz LAN’a katılmak istediğinde radyo NIC için bir şifre gibi belirler. 802.11, ilişkilendirme işlemi ve diğer cihazlarla iletişim sağlayabilmek amacıyla kullanıcının SSID değerinin Şekil 5 ’ten de görüldüğü gibi erişim noktası ile aynı olmasını gerektirir. Aslında SSID opsiyonel güvenlik özelliklerinin yokluğunda erişim noktalarının ilişkilendirme işlemi için gerek duyduğu tek güvenlik mekanizmasıdır.

SSID kullanımı aslında zayıf bir güvenlik mekanizmasıdır. Erişim noktalarının çoğu SSID değerini çerçevelerin içinde her saniye birden fazla kez yayınlarlar. Böylece bir saldırgan kolaylıkla bir 802.11 analiz aracıyla SSID değerini ele geçirebilir. Ek olarak, Windows XP de kullanımda olan SSID ağı koklar (sniffing) ve otomatik olarak son kullanıcının cihazlarındaki radyo NIC’i konfigüre eder.

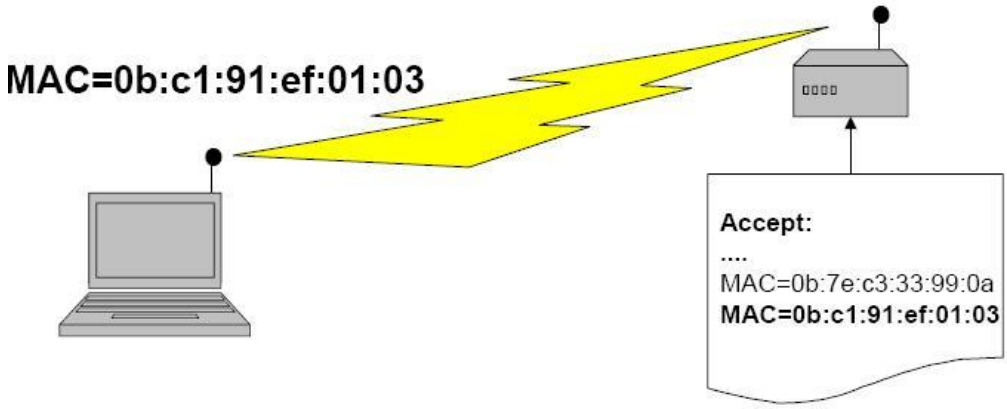


Şekil 5. SSID Kullanımı[8].

Bazı ağ yöneticileri SSID yayınını kapatır fakat, bir saldırgan istasyonların erişim noktası ile ilişkilendirme işlemi sırasında kullandıkları çerçevelerden SSID değerini hala elde edebilir. Bunun için de bir istemcinin ağ ile ilişkilendirilmesini veya tekrar ilişkilendirme işlemini gerçekleştirmesini beklemesi yeterlidir.

1.10.1.2. MAC Adresi Filtreleme

MAC adresi filtreleme işlemi aynı zamanda erişim kontrol listeleri (Access Control List - ACL) olarak da bilinir ve çoğu erişim noktasında bulunan genel bir güvenlik mekanizmasıdır.



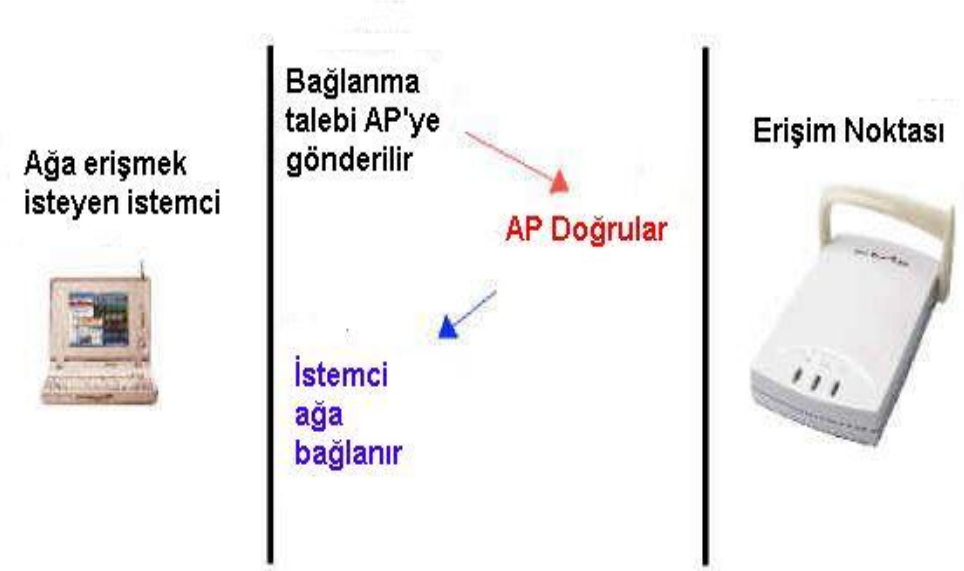
Şekil 6. MAC Adresi Filtreleme İşlemi[8].

MAC adresi filtreleme ağa erişimi belirli MAC adreslerine izin vermek suretiyle sınırlar (Şekil 6). Ancak bu metodun bir çok dezavantajları vardır. Öncelikle istemcilerin MAC adresleri kolaylıkla değişebilir ve böylece yetkisi olan bir istemcinin MAC adresinin erişimi engellenebilir. Ayrıca MAC adresleri düzgün metinler olarak gönderildiği için doğru adreslerin ağdan kolayca yakalanması mümkündür. Diğer bir dezanavantaj ise MAC adres filtrelerinin güncel tutulması ve yönetim işlemlerinin oldukça zor olmasıdır. [8][9]

1.10.2. Doğrulama (Authentication)

1.10.2.1. Açık Sistem Doğrulama (Open System Authentication)

Varsayılan olarak düşünülen doğrulama servisidir. Aslında "sıfır" doğrulama anlamına gelmektedir yani hiçbir doğrulama mekanizması bulunmamaktadır. Şekil 7'nin adımlarında da görülebileceği gibi ağa bağlanmak isteyen her istemciye katılımı için izin verir.



Şekil 7. Açık Sistem Doğrulama[7].

1.10.2.2. Paylaşılan Anahtarlı Doğrulama

Ağa bağlanmayı talep eden istasyonlar ve AP arasındaki doğrulama için aynı gizli (aynı zamanda global) anahtarın paylaşıldığı doğrulama servisidir. Bu anahtar her istasyonun yönetim bilgi birimine (management information base - MIB) sadece yazma özellikli şekilde yazılır ve sadece MAC katmanında kullanılabilir. Bu metot WEP mekanizmasının kullanımını gerektirir.

Şekil 8. Paylaşılan Anahtarlı Doğrulama[7].

Paylaşılan anahtarlı doğrulama beş aşamada meydana gelir: (Şekil 8)

1. Talepte bulunan istasyon AP'ye bir doğrulama çerçevesi yollar
2. AP bu doğrulama çerçevesini alır ve PRNG (Pseudorandom Number Generator) kullanan WEP şifreleme mekanizması tarafından üretilen rasgele bir metinle karşı tarafa cevap verir.
3. Talepte bulunan istasyon bu metini doğrulama çerçevesinin içine kopyalar ve paylaşılan gizli anahtar ile şifreler. Şifrelenmiş çerçeve AP'yeri geri yollanır.

4. Çerçeveyi alan AP metni alır ve aynı gizli anahtar ile deşifreleme yapar. Elde ettiği metni daha önce yolladığı metin ile karşılaştırır

5. Eğer doğru sonucu elde ederse onay yollanır, aksi durumda doğrulama meydana gelmez[7].

1.10. 3. Kabloluyla Eşdeğer Güvenlik (WEP- Wired Equivalent Privacy)

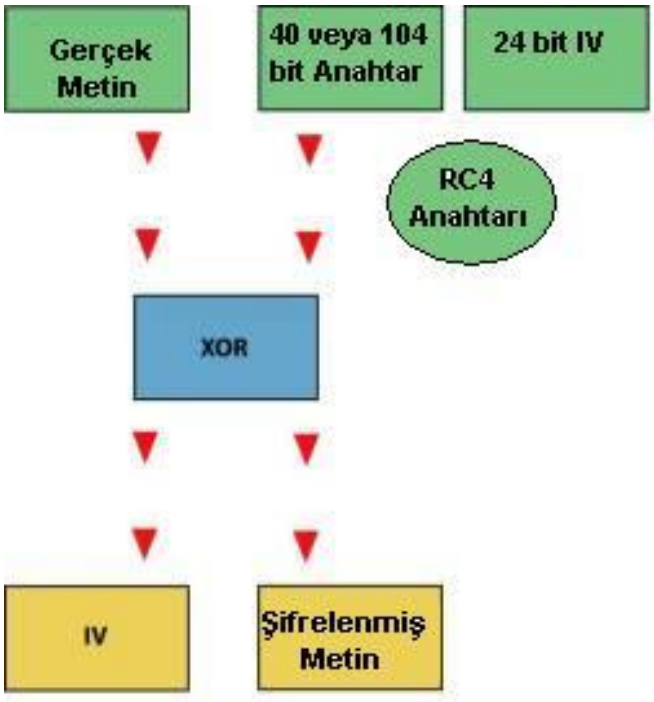
Wired Equivalent Privacy(WEP), orijinal 802.11 güvenlik tanımlamasıdır. Bilgi; ağın kablosuz kısmında ilerlerken, bilgiyi korumak için tasarlanmıştır. WEP, Access pointin ötesinde koruma sağlamaz ve 802.11a, 802.11b, 802.11g ile eşit güvenlik sağlar.

WEP; sadece güvenlik şifreleme metodundan yoksun değil, ayrıca pratik anahtarlama yönetim protokolünden de yoksundur. Gizli anahtar; kimlik denetimi aşamasında, kimliği gösteren belge olarak kullanılabilir. Ayrıca; gizlilik amacı, paketleri şifrelemek için de kullanılabilir. Anahtar AP'e elle girilir ve AP ile haberleşmek isteyen her istemci de bu anahtarı kullanır. Kullanılan ortak anahtarın, bütün kullanıcılar tarafından bilindiği varsayılır. Bu paylaşılmış anahtar, el ile değiştirilene kadar aynı kalır. Otomatik anahtar yönetiminin eksikliği, gizli şifrelenmiş anahtarı açığa çıkarmak ve kullanmak isteyen bilgisayar korsanları için WEP'i kolay av yapmaktadır[11].

WEP'in baslıca üç temel amacı vardır; cihazın kimlik denetimini, gizliliği ve mesaj bütünlüğünü sağlamak. Kimlik denetimi; bir AP'e veri gönderme işlemi olmadan önce yapılmalıdır. Bu kimlik denetimi karşılıklı değildir. Sadece mobil istasyonu, AP ile kimlik denetimi için talepte bulunur, AP karşılık vermez. Kimlik denetimi ikiye ayrılır: Açık Kimlik Denetimi (Open Authentication) ve Anahtar Paylaşımlı Kimlik Denetimi (Shared Key Authentication) Açık Kimlik Denetimi; her kablosuz cihazın, AP ile ilişkiye girmesine izin verir. Anahtar Paylaşımlı Kimlik Denetimi için; AP, mobil istasyona, mesajın içinde bir metin dizgisi gönderir. Mobil istasyon, WEP anahtarını kullanarak dizgiyi şifreler ve bunu AP'e geri gönderir. Mobil istasyon tarafından kullanılan şifreli anahtar; WEP modundayken, düzenli trafik için kullanılan WEP anahtarı ile aynıdır[11].

Önce mobil istasyonun kimlik denetimi yapılmıştır. AP ile ilişki kurmaya hazırdır ve ağdaki diğer elemanlarla veri iletişimini gerçekleştirir. WEP; mobil istasyon ile AP arasında, kablosuz bağlantı üzerinden değiştirilen mesajları, şifreleme yoluyla gizliliği sağlar. Mesajı şifrelemek için, WEP şifreleme algoritması su şekilde çalışmaktadır: Gönderme ünitesi bir başlangıç vektörü üretir. 24 bit'lik başlangıç vektörü (IV), 40 bit'lik

ya da 104 bit'lik gizli anahtara (ortak anahtar) eklenir. Bu anahtar; IV + Gizli Anahtar uzunluğu kadardır (24 + 40=64 bit ya da 24 + 104=128 bit). Oluşan bu yeni anahtar RC4 algoritmasına girdi olur. Bu şekilde, her kullanımda, RC4 algoritmasına farklı bir anahtar girecektir. Daha sonra, RC4 algoritması, sahte rastgele sayı üreteci ile bir akı anahtarı elde eder. Bu anahtarın uzunluğu girdi parametresi kadardır (64 bit ya da 128 bit). Şifrelenmemiş veri, veri bütünlüğü sağlamak için; veri bütünlüğü kontrol algoritmasına sokularak, sağlama bitleri (Checksum - CRC) elde edilir. Bu sağlama bitleri açık verinin sonuna eklenir. Bu veri vektörü (veri + sağlama bitleri - CRC), elde edilen akış şifresi ile XOR işlemine tabi tutularak şifrelenir[11]. Böylece şifreli metin (veri) elde edilir. IV başlangıç vektörü, şifreli metnin basına eklenerek kablosuz ortamdan gönderilir. Bu şifreleme mekanizması sekil 9'da gösterilmiştir.



Şekil 9. WEP Algoritması[10]

WEP'in bütünlük özelliğinin amacı; paket alıcısı için, iletim esnasında paketin gizlice uğraşılıp uğraşılmadığını belirlemektir.

1.10.3 1. WEP'in Zayıflıkları

Daha öncede bahsedildiği gibi WEP; kimlik denetimi, gizlilik ve bütünlüğü sağlamak için tasarlanmıştır ama maalesef bu alanlarda eksikleri vardır. Zayıflığın ilk kaynaklandığı yer, WEP'in anahtar paylaşımlı gizliliği yönetmesindeki eksikliğinden gelmektedir. Bu problem için karşılaşılan en açık sebep, otomatik anahtar yönetiminin eksikliğidir. WEP'in anahtar dağılımı elle yapılır. Her kullanıcı, aynı gizli anahtarı bilmek zorundadır. Geniş kullanıcı topluluğuna anahtar dağılımı yapılır. Bunun değişmesi, her bilinen kullanıcının güncelleştirmeden haberdar edilmesi demektir ve hiç pratik bir durum değildir. Bunun sonucunda, WEP'in kullanıldığı birçok yerde anahtar uzun zaman aynı kalmaktadır. Geniş bir topluluk gizli anahtarı bildiği zaman, anahtarın uzun süre gizli kalması oldukça zordur.

WEP'in diğer bir zayıflığı; gizli anahtarının, ele geçirilmiş paketlerden kolayca çözülmesidir. Çünkü WEP, belirli paket sayısından sonra şifrelenmiş anahtarları yeniden kullanır ve tekrar kullanım meydana geldiğinde dışarıdan olan dinleyicilerin bunu bilmesine izin verir. Herkese duyurma, anahtarın IV kısmından dolayı meydana gelir, şifrelenmemiş olarak gönderilir. Dışarıdan bir dinleyici, anahtarın yeniden kullanıldığı zamanı söyleyebilir.

Anahtarın yeniden kullanıldığı zamanı bilmek; bilgisayar korsanlarına, aynı anahtarla şifrelenmiş çoklu paketleri elde etme izni verir. XOR işlemi boyunca yakalanan mesaj sayesinde, dışarıdan olan dinleyici şifrelenmiş anahtarı yeniden ele geçirebilir. WEP, RC4 algoritmasına, ortak anahtarla beraber IV'yi geçirmektedir. IV değeri her paket için değişmektedir. Başlangıçta sıfır değerindedir ve her isleme girdiğinde değeri 1 artar. Her bir paket farklı bir akış şifresi ile şifrelenir. Belirli bir paket sayısından sonra bütün IV değerleri, dolayısıyla akış şifreleri kullanılmış olacaktır. Bundan sonra RC4 algoritmasının her çalıştırılışında aynı akış şifreleri üretilecektir. Aynı akış şifresi ile şifrelenen mesajlar elde edildiğinde, istatistiksel analiz yöntemleri kullanılarak açık metin elde edilebilir.

WEP anahtarlarının şifrelerini çözmenin ikinci yolu; bir anahtarın kimlik denetim aşamasında kullanıldığı zamandır. 802. 11 iki kimlik denetimi modu tanımlar; Anahtar Paylaşımlı (Shared Key) ve Açık Kimlik Denetimi (Open Authentication). Anahtar paylaşımlı kimlik denetimi kullanıldığında; kimlik denetimi için kullanılan anahtar, paket

şifrelemesi için WEP tarafından kullanılan anahtar ile aynıdır. Böylece sifreyi ele geçirmek daha da kolaylaşır.

WEP anahtarlarının ortaya çıkmasına neden olan üçüncü yol; RC4 algoritmasının, anahtar üretim algoritmasının zayıf anahtarlar üretmesidir. Bu zayıf anahtarlar tespit edilerek, anahtarların ilk önce başlangıç bitleri, daha sonra ardışık şekilde diğer kısımları çözülebilmektedir.

1.10.3. 2. Dinamik Anahtar Değişimi (Dynamic Key Exchange- DKE)

DKE; birçok kurulusun WEP'deki otomatik anahtarlama yönetiminin eksikliğinin üstesinden gelmek için, kablosuz güvenliği geliştirmek adına ilgilendiği bir çalışmadır. DKE için iki temel olumsuzluk vardır: Birlikte islerlik yoktur ve bütün uyarlamalar AAA (Authentication, Authorization Accounting) hizmet sağlayıcısı gerektirir. Bunun anlamı; küçük bölgeler ve SOHO (Small Office Home Office) ağlar için bir çözüm sağlamaz. Birlikte çalışabilirliğin önemli olmadığı ve sadece AAA hizmet sağlayıcısının olduğu durumlarda DKE kullanılabilir.

1.10.4. 802. 11i

WEP'in eksikliklerini gideren, 802. 11'in çözümü Sağlam Güvenli Ağ'dır (Robust Security Network- RSN). RSN, 802. 11 Görev Grubu "i" tarafından geliştirilmiştir. RSN; kablosuz paketin şifrelenmesi için İlerlemiş Şifreleme Standartı (Advanced Encryption Standart- AES) tabanlıdır. Kimlik denetimi, yetkilendirme ve anahtar yönetimi için 802. 1X tabanlıdır. AES; bilinen kusuru olmayan, çok güçlü bir şifreleme algoritmasıdır. Şimdiye kadar, şifre çözümleyicilerin her çeşidine karsı dirençli olmuştur. Ancak AES, sayısal olarak yoğundur ve su an piyasada olan birçok AP'in sayısal mevcut gücünün çoğunu tüketebilir. Giriş düzeyindeki PDA'ların, AES'i desteklemek için gerekli sayısal gücü olmayabilir.

WEP'in açıklarını gidermek için geliştirilen bu protokol ile aşağıdaki özellikler sağlanmaktadır:

- Kimlik denetimi (Authentication),
- Şifreleme (Encryption),
- Yetkilendirme (Authorization),

• Anahtar Yönetimi,

• Her paket için şifreleme yapılmaması,

• Gizlilik ve mesaj bütünlüğü için güçlü bir şifreleme algoritmasının kullanılması,

• Korunmamış bilgilerin gönderilmemesi ve alınmaması,

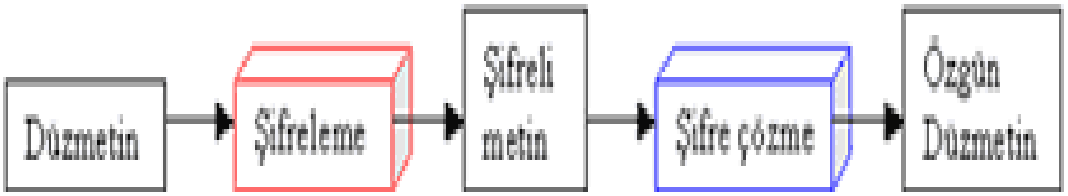
• Mesajlara sıra numarası konulması,

• Mesajın kaynağının asıllanması.

802. 11i standardı, veri güvenliği için yeni bir şifreleme algoritması kullanmakta, anahtar yönetimini dinamik bir şekilde yapmakta ve yetkisiz kullanıcıların ağa girişini engellemek için kimlik denetimi sunucusu ile asılama yapmaktadır. Kullanıcılara ağa ulaşmadan önce kimlik denetimi yapılmakta, bu işlemden sonra üretilen oturum anahtarları dağıtılmakta, bu anahtarlar kullanılarak üretilen yeni anahtarlar ile güvenli veri transferi yapılmaktadır.

1.10.4. 1. Gelişmiş Şifreleme Standardı (Advanced Encryption Standart- AES)

Bu standart; şimdiki Federal Information Processing Standart (FIPS) şifreleme tanımlaması olan, DES'in (Data Encryption Standart) yerine tasarlanmıştır. AES; devlet için zorunlu, endüstri için isteğe bağlıdır. AES, Rijndael şifreleme algoritmasını kullanır. Bu algoritma yüksek güvenlik ve hızlı şifreleme gerektiren pek çok uygulamada kullanılmaktadır. 128, 192 veya 256 bitlik anahtarlar kullanıp, 128, 192 veya 256 bitlik blok şifreleme yapabilmektedir. NIST'in (National Institute of Standarts and Technology), AES geliştirme çabaları için yapılan algoritmalarından seçilen bir şifreleme algoritmasıdır. AES; şimdiye kadar bilinen bir kusuru olmayan ve bütün şifre çözücülere karsı direnen çok güçlü bir şifreleme algoritmasıdır. AES'in yüksek sayısal gereksinimleri vardır (WEP'den daha yüksek) ve ağ bileşenlerinde yer alan donanımın yardımına ihtiyacı vardır. Bir şifreleme algoritması olarak AES'in kullanımı, sayısal olarak yeterli AP'lerin kullanımını gerektirir. Mobil istasyon alanında, diz üstü bilgisayarlar AES'nin arttırılmış sayısal ve güç isteklerini karşılayabilirler ama başlangıç seviyesindeki çok gelişmemiş PDA'lar bu istekleri karşılayamazlar.



Şekil 10**.** Şifreleme ve şifre çözme işlemleri diyagramı[26].

Şifreleme işleminde düz metin, şifreleme işlemine tabi tutulur ve bu işlem sonucunda elde edilen şifrelenmiş veri alıcı tarafa yollanır. Alıcı taraf şifrelenmiş veriyi şifre çözme işlemi ile düz metin haline çevirir[26].

1.10.4. 1. 1 AES Algoritmasının Yapısı

AES Algoritması genel olarak tur işlemlerinin ve tur işlemlerinin içerisinde gerçekleştirilen tur dönüşüm işlemlerinin bir bütünü olarak düşünülür.

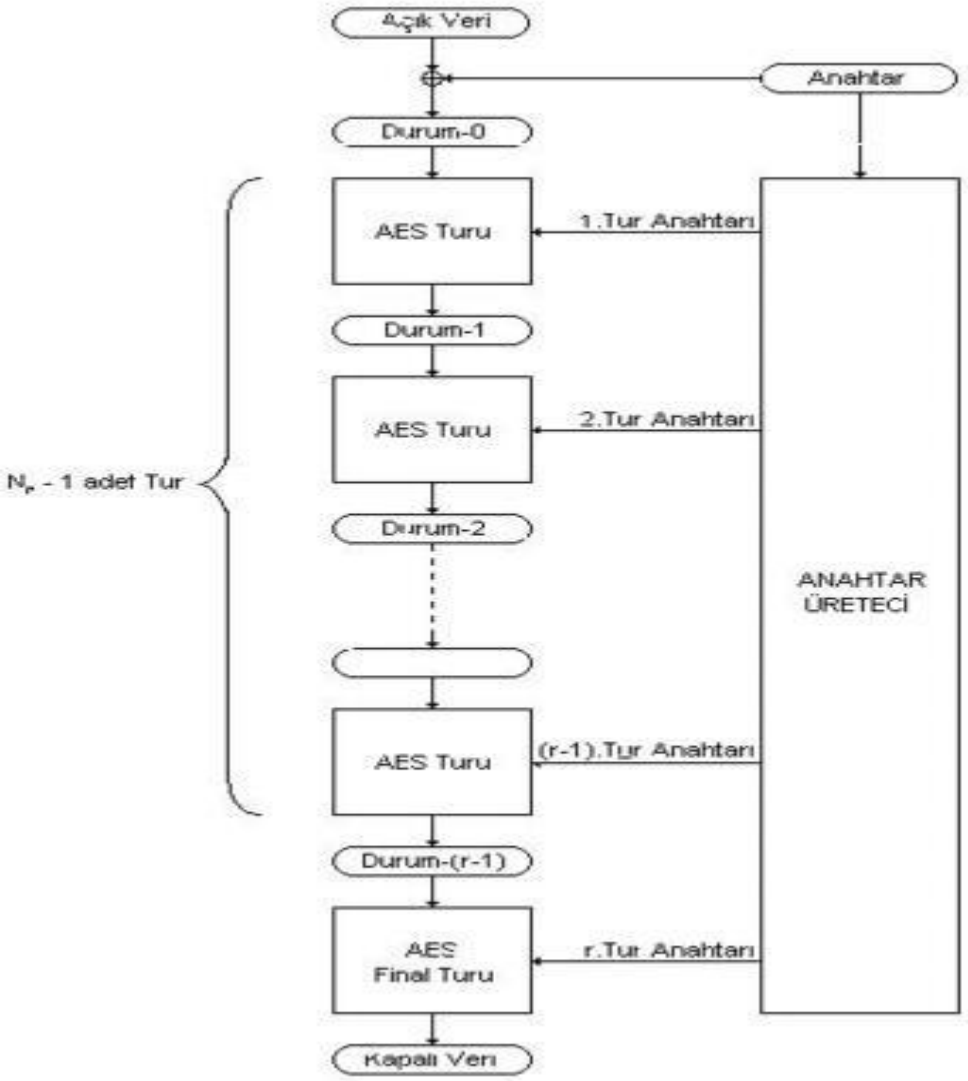
AES algoritması 128 bit veriyi şifrelemek ve çözmek için oluşturulmuş simetrik veri kodlama standardıdır.

Matris 4 satır, 4 sütun olmak üzere 16 bölmeden oluşur. Bu matrise “durum” denilir.

Durumun her bölmesine 1baytlık veri düşer. Her satırda 32 bitlik bir kelimeyi meydana getirir. Bu gösterimde, Nk=4 olmaktadır.

AES-126 10 çevrimdir. İlk olarak 128 bitlik anahtar on çevrimde farklı şekliyle kullanılması amacıyla genişletilir [27]. Daha sonra Tur Anahtarını Ekleme adımı gerçekleşir. Bu aşamadan sonra 10 çevrim gerçekleşir. Her çevrim sırasıyla Bayt Değiştirme, Satırları kaydırma, Sütunları karıştırma ve Tur Anahtarını Ekleme işlemlerinden oluşur. Son çevirim olan onuncu çevrimde Sütunları Karıştırma adımı uygulanmaz [29].

AES blok şifreleme algoritmasının blok diyagramı Şekil 11’de verilmiştir [28].



Şekil 11**.** AES blok diyagramı[28].

1.10.4.1.1.1. Bayt Değiştirme

İlk olarak 128 bitlik veri 8'er bitlik 16 parçaya ayrılır ve 4x4 boyutundaki durum matrisi oluşturulur (bkz. Şekil 12) [27]. Tüm işlemler bu durum matrisi üzerinden gerçekleşmektedir. Bayt değiştirme adımında her 8 bitlik parçaya matematiksel bir dönüşüm uygulanır. Bu dönüşüm iki aşamada gerçekleşir. İlk olarak indirgeme polinomu P(X)=X8+X4+X3+X+1 kullanılarak çarpmaya göre ters alma işlemi uygulanır. Buradan elde edilen sonuç bir geçiş matrisi ile çarpılarak sabit bir matris ile toplanır [27]. Bu

işlemlerin sonucunda bayt değiştirme adımı sonucu elde edilir. Bu işlemlerin sonuçları Şekil 13'de tablo olarak verilmiştir. Bu dönüşümler 8 bitlik 16 veriye seri olarak tekrarlandığında 128 bitlik veri bu adımdan geçmiş olur.

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$

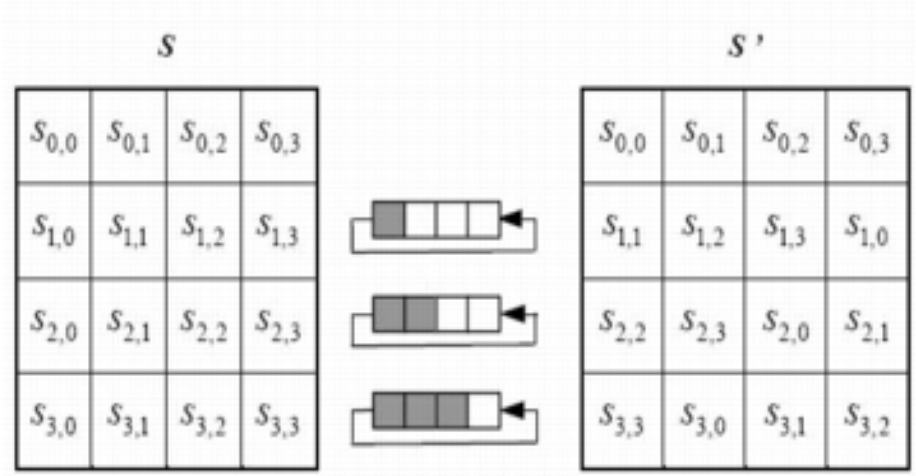
Şekil 12. Durum matrisi[27].

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7c	77	7b	f2	6b	6f	C5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
A	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
B	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
C	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
D	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
E	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
F	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Şekil 13: S-kutusu çıkışları[27].

1.10.4. 1.1.2. Satırları Kaydırma

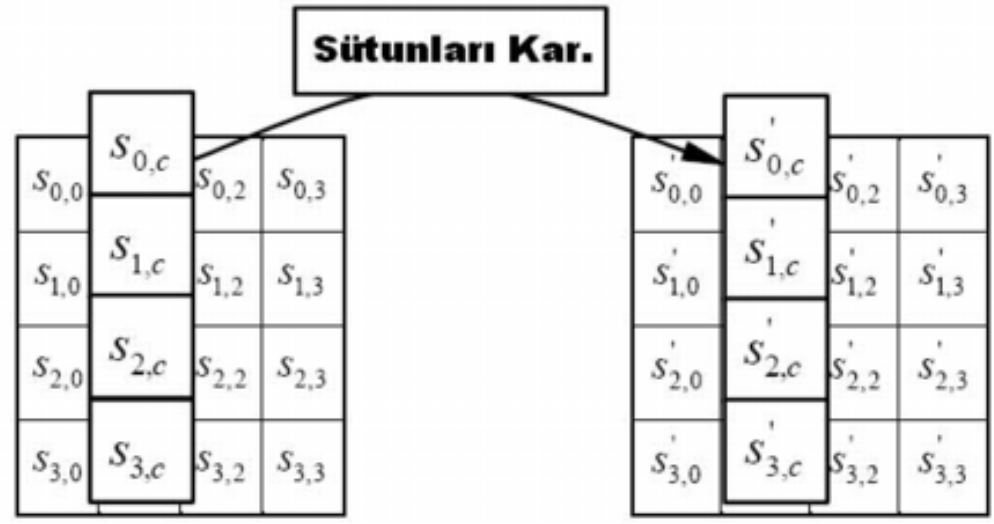
Bu adımda Bayt Değiştirme işleminden elde edilen veri yine 8'er bitlik 16 parçaya ayrılır ve 4x4 boyutunda bir matris haline getirilir. Martisin ilk satırı sabit bırakılarak ikinci, üçüncü ve son satırlar sırasıyla bir, iki ve üç kere sola kaydırılır ve bu işlemler sonucu yeni bir 128 bitlik veri elde edilir. Bu işlem blok diyagram halinde Şekil 14'de gösterilmektedir.



Şekil 14. Satırları kaydırma[27].

1.10.4. 1.1.3. Sütunları Karıştırma

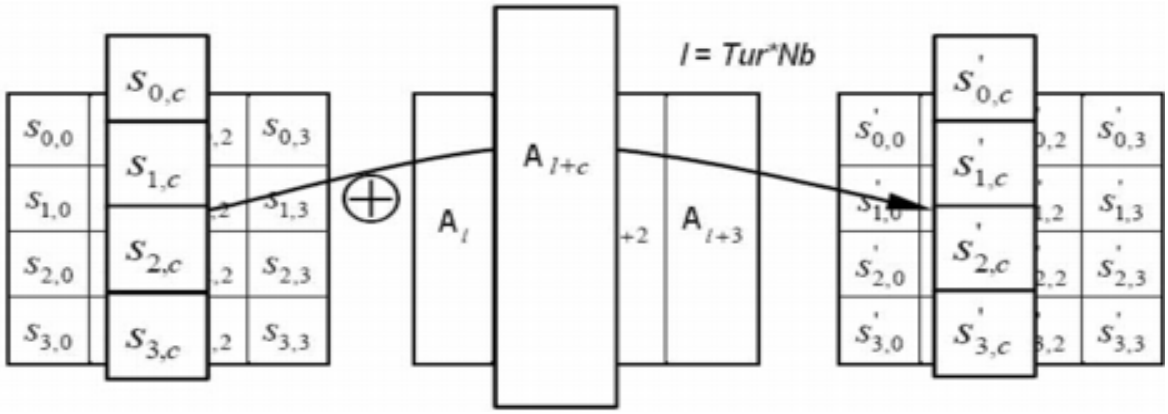
Süt Satırları Kaydırma adımında oluşan 128 bitlik verinin 8'er bitlik 16 parçasının herbiri belirli işlemlere tabi tutularak yeni bir 128 bitlik veri elde edilir (bkz: Şekil 15). Bu adımda işlemler durum matrisindeki her bir sütun üzerinde bağımsız olarak gerçekleşir. Her bir sütun bir polinom olarak düşünülerek a(X)={03}X3+{01}X2+{01}X+{02} polinomu ile modülo X4+1'de çarpma işlemi gerçekleştirilir [28]. Sütunları kaydırma işleminin diyagramı Şekil 15'de verilmiştir.



Şekil 15. Sütunları karıştırma[27].

1.10.4. 1.1.4. Tur Anahtarını Ekleme

Bu aşamada bir önceki işlemin sonucunda elde edilen 128 bitlik durum matrisi ile genişletilen anahtarın o çevrimle ilgili bölümü olan 128 bitlik anahtar dizisi exorlanır. Bu aşama Şekil 16'da verilmiştir [27].



Şekil 16. Tur anahtarını ekleme[27].

Bu işlemler her tur için tekrarlanır ve turlar bittiği zaman, veri şifrelenmiş olarak değişir. Şifrenin çözülmesi için ise işlemler geriye doğru uygulanır.

1.10.4. 2. Geçici Anahtar Bütünlüğü Protokolü (Temporal Key Integrity Protocol –TKIP)

TKIP; WEP'in zayıflıklarını adreslemek ve var olan donanımı kullanarak daha güvenli WLAN için bir çözüm yolu sağlamak için geliştirildi. TKIP; WEP'den daha fazla hesaplama gücü gerektirir ama AES tabanlı RSN ve WPA2'den daha az hesaplama gücü gerektirir. TKIP, yazılımı geliştirmek için uygulanabilir. TKIP, RC4 algoritmasını kullanır (WEP ile aynı algoritma), ek olarak sağladığı güvenlik özellikleri şunlardır:

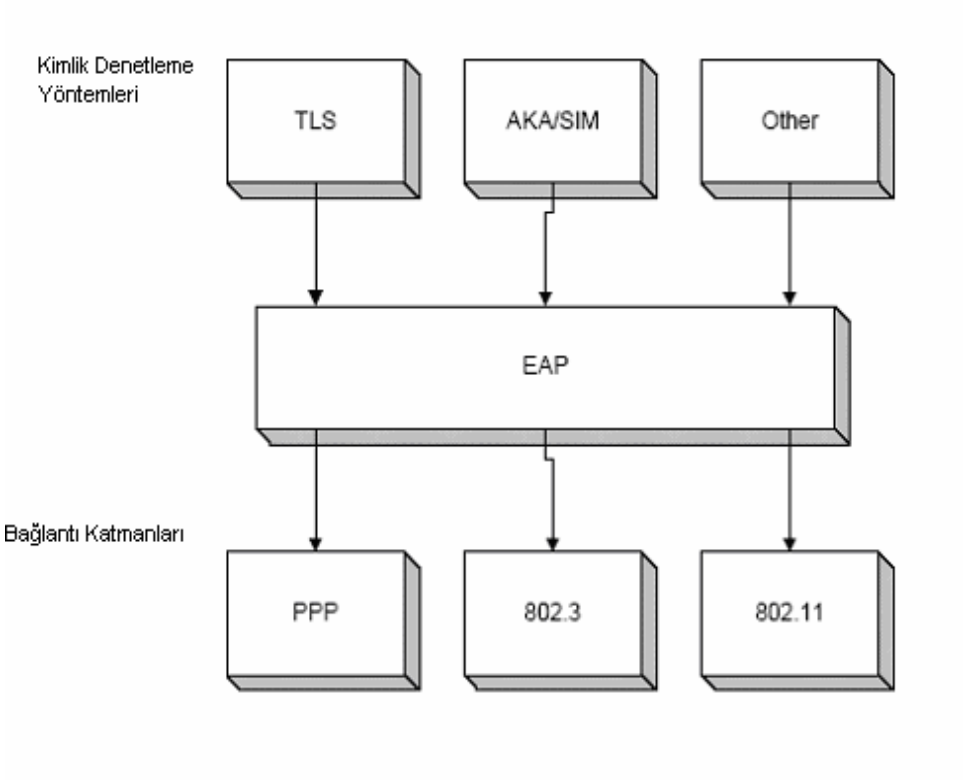
- Her pakete yeni anahtar karıştırma fonksiyonu
- Michael olarak adlandırılan yeni mesaj bütünlük kontrolü
- Daha uzun başlangıç vektörü (WEP'de 24 bitken TKIP'da 48 bittir)
- Anahtarları yenileme mekanizması

TKIP'da veri bütünlüğünü sağlamak için Michael algoritması kullanılır. Michael veri bütünlük kodu, kaynak ve varış MAC adreslerini ve veriyi alarak sağlama bitleri (checksum) oluşturur. Bu bitler verinin sonuna şifrelenerek eklenir. Böylece mesaj içeriğinin değiştirilmesi önlenir. WEP'in tersine, alıcı ve vericinin adresleri açık şekilde gönderilmez.

TKIP bir oturuma; iletilen her 10,000 paketten sonra değişen, mobil istasyonun ve AP'in bildiği 128 bit geçici anahtarla baslar. Oturum anahtarı, her paket anahtarını üretmek için temel olarak kullanılır. Her paket anahtarı; geçici oturum anahtarı, mobil istasyonun MAC adresi ve IV'ı kullanan bir birleşim fonksiyonunu kullanarak üretilir.

1.10.4. 3. Kimlik Denetimi Paket Akısı –EAP

Extensible Authentication Protocol (EAP), geniş bir kimlik denetimi protokolü çeşitliliğini içeren, bir genel kimlik denetleme paket akısıdır. Sekil 10'da EAP paket akısının blok diyagramını göstermektedir. EAP, PPTP (Point to Point Tunneling Protocol) ile kullanım için geliştirilmiştir. 802. 1X; EAP'ı kablosuz ağ için, ağının giriş kontrol mekanizmasının bir parçası olarak kullanmaktadır. Buna göre, EAP data bağlantılarını geniş bir çeşitliliğinin üstünde kullanılabilir.



Sekil 17. Kimlik denetimi paket akısı diyagramı[14].

1.10.5. EAP Kimlik Denetleme Yöntemleri

EAP; çoklu kimlik denetleme protokol seçimini destekleyen bir paket akısıdır Kimlik denetimi için kullanılan mevcut protokol, mobil istasyonu ile AP arasında görüsme işlemi boyunca seçilir. Es cihazlar, kimlik denetleme yönteminin seçimini protokol tabanlı yaparlar.

1.10.5. 1. MD5 – Message Digest 5

MD5, EAP kimlik denetleme yöntemlerinin en basitidir. Kablosuz ağlarda kullanıldığı zaman, en az güvenli olanıdır. MD5; istemciden (mobil istasyon) ağa (AP) tek yönlü bir kimlik denetleme yöntemidir. MD5'in asıl eksikliği; kimlik denetleyicisine giriş ve tek yönlü bir kimlik denetleme yöntemi için açık metin modunda şifreyi içermesidir. Sadece mobil istasyonunun şifreyi bırakırken ortadaki adam saldırısından (man-in-the–middle attack) etkileneceği ispatlanmıştır. MD5, anahtar yönetimini desteklemez. Bu yüzden saldırganlar, WEP anahtarlarının şifresini kırabilirler.

1.10.5. 2. LEAP – Lightweight EAP

LEAP; Cisco tarafından geliştirilen, çift yönlü kimlik denetimini destekleyen bir EAP kimlik denetleme yöntemidir. RADIUS (En yaygın kullanılan kimlik denetleme sunucusu) sunucusu yolu ile kimlik denetimi için; kullanıcı adı ve şifresini ve AP kimliğini kullanır. Kimlik denetimi üzerine; LEAP, oturum kullanımı için tek zamanlı WEP anahtarları üretir. LEAP kullanarak, her kullanıcı kablosuz ağa farklı WEP anahtarı kullanarak bağlanır. Oturum anahtarları, kullanıcının yeniden log-in olmasına neden olan RADIUS zaman asımı özelliğini kullanarak yenilenebilir. Yeniden log-in olma, kullanıcının bilgisi ve müdahalesi olmadan meydana gelebilir. LEAP'ın saldırılara açık olması, çift yönlü kimlik denetimi için MS – CHAPv1 protokolünü kullanıyor olmasından gelmektedir. LEAP'ın eksikliği; sadece Cisco tabanlı ağlarda uçtan uça (end to end) çalışıyor olmasıdır.

1.10.6. WPA (Wi - Fi Protected Access)

WEP algoritmasının açıklarını gidermek için IEEE çalışma grupları tarafından çalışmalar yapılmış ve biri kısa vadeli diğeri ise uzun vadeli olmak üzere iki farklı çözüm üretilmiştir. Uzun vadeli olan çözüm IEEE'nin "i" çalışma grubu tarafından tam olarak güvenli bir protokolün oluşturulması şeklindedir. Bu çalışmalar esnasında sektörün WEP algoritmasındaki güvenlik zaaflarından etkilenmemesi ve biraz

da olsa güvenlik önlemlerinin arttırılması için WEP algoritmasının eksik yönlerinin geçici yöntemlerle giderilmesi için Wi-Fi grubu ve IEEE tarafından WPA geliştirilmiş ve sektör için geçici bir çözüm üretilmiştir. WPA'nın geliştirilmesiyle eski donanımın sadece yazılım güncelleştirilmeleri yapılarak kullanılabilmesi sağlanmıştır. Var olan donanımın kullanımı ile WPA'nın kullanımının daha kolay bir şekilde ve daha hızlı bir şekilde yayılması sağlanmıştır.

WPA, IEEE 802.11i standartına dayanmaktadır. Onun özelliklerinden bir kısmını barındırmaktadır. WPA'nın iki farklı modu bulunmaktadır. Normal ve tam modu ufak değişikliklerle 802.1X doğrulama ve erişim kontrolü mekanizmasını kullanır. Diğer mod olan WPA-PSK ise ön paylaşımlı anahtar kullanır ve Radius gibi anahtar dağıtımı görevini yapan sunucuların yönetimi için yeterli kaynakların olmadığı SOHO (Small Office Home Office) ortamlarında kullanılabilir.

WPA'da kullanılan şifreleme algoritması tıpkı WEP gibi RC4 algoritmasına dayanan Geçici Anahtar Bütünlük Protokolü (Temporal Key Integrity Protocol - TKIP) 'dür. TKIP WEP'ten farklı olarak önemli bazı değişiklikler içermektedir. IV'nin uzunluğu 24 bitten 48 bite çıkarılmıştır ve şifreleme anahtarları her oturumda değiştirilmektedir. Ayrıca her paket için farklı anahtar kullanımını sağlamak amacıyla da bir anahtar karıştırma fonksiyonu (key mixing function) kullanılmaktadır. WPA iletim sırasında verilerin değişikliğe uğramamasını sağlamak amacıyla da Michael adı verilen bir mesaj bütünlük kodu (message integrity code - MIC) kullanır[12].

1.10. 6. 1. WPA Kullanıldığı Zaman Göz Önüne Alınması Gereken Konular

WPA içeriğinin kullanımı sırasında, göz önüne alınması gereken konuların bazıları aşağıdaki gibidir:

• İstasyonlar için yazılım geliştirme gereksinimi vardır.

• WPA, ön kimlik denetimini desteklemez.

• WPA ile başıboş dolaşmak mümkün değildir. İstasyonlar yeniden kimlik denetimi yapmalıdır. Bu, 600 milisaniye sürer.

• Yeni istemci kapasitesi isteği (802. 1X ve WPA) vardır.

• İstasyonlar ve AP için yazılım geliştirme isteği vardır[11][12].

1.10.7. WPA2 (802.11i)

TGi tarafından kablosuz ağların güvenliği için uzun vadeli çözüm olarak düşünülen WPA2 Mayıs 2004 tarihinde standart haline gelmiş ve Ekim 2004 tarihinden itibaren de bu protokolü destekleyen ürünler üretilmeye başlanmıştır.WPA2 ayrıca IEEE 802.11i olarak da adlandırılmaktadır. WPA günümüzde kırılmamış olsa da WEP tabanlı bir yapı olduğu ve eksiklerinin çıkabileceği şüphesinden dolayı (RC4 algoritmasının zayıflıkları) IEEE tarafından geliştirilen bu protokol WPA'nın aksine WEP üzerine kurulmamış, yeni ve farklı bir yapı olarak geliştirilmiştir. WPA2'nin WPA ve WEP'ten en büyük farkı ağ trafiğini şifrelemek için RC4 algoritmasını değil AES (Advanced Encryption Standart) [13] algoritmasını kullanmasıdır.

AES kullanımı, Wi-Fi ağları uzun dönemde çok daha fazla güvenilir hale getirecektir. Fakat WPA'dan WPA2'ye geçişte donanım değişikliğini gerektirmektedir ve WPA gibi mevcut ürünler üzerinde yapılacak yazılımsal değişiklik ile geçiş mümkün değildir.

WPA2 WEP'i artık geçerli bir güvenlik mekanizması olarak görmediği için sadece WPA'yı desteklemekte, WEP'i desteklememektedir. WPA2 doğrulama ve anahtar yönetimini IEEE 802.1X standardı ile gerçekler. Veri bütünlüğü MIC ile sağlanır. WPA2'de şifreleme AES tabanlı Counter Mode with CBC-MAC Protocol (CCMP) ile gerçeklenir. CCMP'de de IV kullanılır ve uzunluğu 48 bittir. IV, paketlere sıra numarası vermek için kullanılır. Bu paket numarası daha sonra, diğer bilgilerle beraber hem mesaj bütünlük kodu (MIC) oluşturmak, hem de paketi şifrelemek için AES şifreleme algoritmasında parametre olarak kullanılır.

WPA2 gezginliğe destek vermektedir. Gezginlik özellikle gerçek zamanlı iletişimlerde veri kaybını önlediği için önem kazanır. WPA2 gezginliği iki farklı şekilde gerçekler:

• Önceden Doğrulama: Önceden doğrulamada 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 işlemleri tekrar yapılmaz

•Anahtar önbellekleme: Erişim noktası ile daha önceden anahtar belirleme işlemi gerçekleşmiş ise bu anahtarlar bellekte saklanır. Bu erişim noktası ile iletişime geçildiğinde 802.1X işlemleri tekrar yapılmaz[11][12].

1.10.7.1 WPA2 Kullanıldığı Zaman Göz Önüne Alınması Gereken Konular

WPA2 içeriğinin kullanımı sırasında göz önüne alınması gereken konuların bazıları aşağıdaki gibidir:

• Hızlanmış AES için donanım gereksinimi. Bu yeni APler ve bazı durumlarda yeni NIC/kablosuz istemci donanımını gerektirir.

• Yeni istemci kapasiteleri gereksinimi[11][12].

Özellik	WEP	WPA	WPA2	802.11i (RSN)
Giriş kontrolü	Yok	802.1x	802.1x	802.1x
Kimlik Denetimi	Yok	EAP	EAP	EAP
Şifreleme Algoritması	RC4	RC4	AES	AES
Anahtar bit uzunluğu	40 bit veya 104 bit	128 bit şifreleme, 64 bit kimlik denetimi için	128 bit	128 bit
Paket Anahtarı	Birbirine bağlı	Karışık fonksiyon	İhtiyaç yok	İhtiyaç yok
Anahtar Yönetimi	Statik	802.1X + TKIP	802.1X + CCMP	802.1X + CCMP
Anahtar Ömrü	24 bit IV	48 bit IV	48 bit IV	48 bit IV
Kimlik Denetleme Yöntemleri	Anahtar Paylaşımlı	Anahtar Paylaşımlı,EAP-tabanlı yöntemler	Anahtar Paylaşımlı,EAP-tabanlı yöntemler	Anahtar Paylaşımlı,EAP-tabanlı yöntemler
Başlık Bütünlüğü	Yok	Michael	Michael	CBC-MAC
Bilgi Bütünlüğü	CRC32	Michael	Michael	CBC-MAC
Ön Kimlik Denetimi	Hayır	Hayır	Hayır	Evet
Dolaşım	Sınırlı	Sınırlı	Sınırlı	Evet

Tablo2: WEP, WPA, WPA2 ve IEEE 802. 11i'nin karşılaştırılması[14]

Tablo 2'de, WEP, WPA, WPA2 ve IEEE 802. 11i güvenlik standartlarının birbirleri ile karşılaştırılması gösterilmektedir.

1.11. VoIP (Voice over IP)

Bundan 20-30 yıl öncesine kadar, yani internet henüz yokken interaktif iletişim sadece PSTN Public Switched Telephone Network/ genel anahtarlamalı telefon ağı) hatlı telefonlarla yapılabiliyordu. Veri iletimi özellikle uzun mesafeler için oldukça pahalıydı. Ve henüz kimse görüntülü iletişimi hayal bile edemiyordu.

PSTN şebekeleri kullanıcılara her çağrı için bir uçtan bir uca bir devre bağlantısı sağlarlar. Arayan ve aranan tarafların numarasına göre, arayan tarafın bağlı olduğu santralden başlayarak, aradaki santraller ve diğer uçtaki santrale kadar bir devre kurulmaktadır. Bu santraller arsındaki sinyalleşme temel olarak çağrı kurma, çağrı önlendirme ve çağrı sonlandırma işlemlerinden oluşmaktadır. PSTN hizmeti yaklaşık yüz yıldan bu yana devam etmiştir.

Ancak buna paralel olarak veri trafiği için ayrı şebekeler oluş muş tur. Doğal olarak ayrı ses ve veri şebekeleri servis sağlayıcı için ilave yük aboneler için de ilave ücret anlamına gelmektedir. PSTN trafiği her geçen gün daha fazla veri içerikli olamaya yüz tuttukça ses ve veri şebekelerinin birleşmesi yani tek bir platforma indirgenmesi ihtiyacı daha fazla belirgin hale gelmiş tir. Bu nedenle internet servis sağlayıcıları ve ekipman üreticileri IP temelli olarak ses/veri iletimine yönelmişlerdir

1995'lerde modemlerin 14,4 kbps(kilo bit per second) hızına erişmesi, aynı anda 8 kbps'lik low speed codec'lerin (orjinalinde GSM(Global System for Mobile Communication) için geliştirilmiştir) kullanılabilir hale gelmesiyle IP ağları üzerinden ses transferi teknik olarak mümkün hale geldi. 1995te ilk küçük VOIP uygulaması ortaya çıktı. Uygulamalar yaygın olarak kullanılmamakla birlikte standartlaştırma çalışmaları da aynı yıl başlamıştı. 1996'da ilk VOIP standartları kabul edildi.Düşük kapasiteli H.323 geçitleri(gateway) gibi ilk öncü ürünler aynı yıl geliştirildi. Geçitlerin ortaya çıkması ve kullanımı VOIP tarihinde anahtar bir rol oynamıştır

Geçitler bilindiği üzere iki farklı tip ağ arasına iletişimi sağlamak için kullanılırlar.Kendi aralarında birbirlerinden oldukça farklı protokollerle konuşan iki ağı birleştirmek, konuşturmak ve birinden diğerine veri akışını sağlamak gibi zor bir görev üstlenmişlerdir.) Nihayetinde bütün bu geliş meler ilk internet üzerinden telefondan telefona görüşme ile sonucunu verdi.

İnternet ve intranetlerin geliş erek yaygınlaşmasıyla birlikte ses iletişiminin paketlenerek, analog teknolojilere göre daha avantajlı olan IP ağları üzerinden iletimi günümüzde son derece ekonomik ve cazip görünmektedir. Nitekim paketlenerek IP trafiği üzerine oturtulmuş ses verilerinden oluşan telefon faturaları, özellikle deniz aşırı konuşmalar dikkate alındığında ciddi bir ucuzlama sağlıyor. Bunun yanı sıra VOIP gerçekleştirimi için özel cihazlara ihtiyaç duyulmamaktadır. Genel amaçlı bir kişisel bilgisayar, seskartı, mikrofon, speaker ve birkaç özel yazılım bilgisayardan bilgisayara arama yapmak için yeterlidir. Bu ekipmanlar da zaten çoklu-ortam destekli günümüz bilgisayarlarının hemen hemen hepsinde bulunmaktadır.

1.11.1. Devre Anahtarlama ve Paket Anahtarlama (Circuit Switching vs Packet Switching)

PSTN ve IP network farklı iki teknoloji olan devre anahtarlama(PSTN) ve paket anahtarlamaya(IP network) dayandığından dolayı her iki teknolojiyi de incelememiz; PSTN'de sesin nasıl taşındığını ve iyi kalitede hizmetin neden devre anahtarlama yöntemi ile elde edilebileceğinin anlaşılması sağlayacaktır. Böylece ses sinyallerinin IP ağı üzerinden iletiminde ne gibi problemlerle karşılaşabileceğimize dair daha iyi bir görüş açısına sahip olabileceğiz.

1.11.1.1. Devre Anahtarlama Ağı (Circuit Switching Network)

Devre anahtarlama ağında iletişim bağlantı tabanlı bir şekilde kurulmaktadır. Devre anahtarlamada tüm görüşme için tek bir bağlantı kurulur. Yani iki nokta çift yönlü olarak bağlanır ve bu bağlantı "devre " olarak adlandırılır.

Herbir aramada üç farklı evre meydana gelmektedir:

1) Yol kurulması (path set-up) **:** Sinyalleme mekanizması kullanılarak 64 kbps'lik sabit bir yol kurulur.
2) İletişim (communication) :Yol bir kere kurulduktan sonra iletişim başlar.
3) Yolun serbest bırakılması (path release):İletişim tamamlandıktan sonra yol ve kullanılan tüm kaynaklar serbest bırakılır.

Tipik bir telefon görüşmesinin aşağıdaki gibi gerçekleşir:

- Telefonunuzun ahizesini kaldırıp çevir sesini duyarsınız. Bu, telefon şirketinizin yerel şubesi ile bağlantıda olduğunuzu bilmenizi sağlar.
- Aramak istediğiniz kişinin telefon numarasını çevirirsiniz.
- Arama, yerel taşıyıcınızda bulunan anahtar üzerinden aradığınız kişiye yönlendirilir ve sizin telefonunuzla aradığınız kişinin hattı arasında bir bağlantı kurulmuş olur. Bu durum devrenin açılmasıdır.
- Görüşmenizi yaparsınız.
- Telefonunuzu kapatırsınız. Telefonu kapattığınızda devre de kapanır ve hattınız boş alır.

10 dakika konuştuğunuzu farzedelim. Bu süre boyunca iki telefon arasında kurulmuş olan devre sürekli açık kalır. Geleneksel PSTN üzerinden gerçekleştirilen telefon görüş meleri her iki yönde 64 kbps (toplamda 128 kbps) veya 1024 kbps (toplamda 2048 kbps) gibi sabit bir oranda iletilirler. Bir kilobyte'da 8 kilo bit olması, her bir saniyede 16 KB verinin iletilmesi anlamını taşır ki bu da her bir dakikada 960 KB'ye tekabül eder. Bu durumda 10 dk'da yaklaşık 9,4 MB veri iletilmiş olur.

Tipik bir telefon görüşmesine bakılacak olunursa iletilen verinin büyük bir kısmını israf olduğu görülür. Çünkü siz konuş urken karşı taraf sizi dinlediği için bağlantının yarısı kullanımdadır ve bağlantının 4.7 MB'lık kısmı boşa harcanır. Bunun yanı sıra birçok konuşmanın önemli bir kısmında ne siz ne de karşı taraf konuşur. Görüldüğü üzere her iletişim kurulduğunda 64 kbps'lik bantgenişliği sabit olarak ayrılmaktadır. Kullanıcı daha az ya da daha fazla bantgeniş liği talep edememektedir. Sessiz periyotlar da bile kaynaklar tamamıyla kullanılır durumda kalır. Bu da kullanılmayan kaynakların kullanılmayan kapasitesi anlamını taşır. Yani devre anahtarlama yöntemi bu kullanılmayan kapasiteyi esnek bir trafikle doldurma yetisine sahip değildir.

Devre anahtarlama yönteminin en önemli avantajı ise ayrılmış olan bant genişliğine (bandwidth:bir bağlantıdan yollayabileceğimiz bilgi miktarı) uygun olarak tüm konuşma süresince aramanın kalitesi önceden bilinebilmesidir.

1.11.1.2. IP Ağı (IP Network) :

Voice Over IP'de ses verileri PSTN'in geleneksel devre tabanlı protokollerinden farklı olarak ayrık paketler halinde taşınır.

IP ağda devre anahtarlamada olduğu gibi bir bağlantının kurulması gerekmezken hiçbir kaynak tahsisi de söz konusu değildir.Bağlantı zaten halihazırda IP tarafından sağlanmış durumdadır .Bir VOIP araması başlatıldığında ilk olarak standart telefon sesi paketlere çevrildiği IP platformuna geçer.Bu platform bir PC ya a gateway olabilir. Bir kez sıkıştırıldıktan sonra bu paketler kaynakla hedefi bağlayan bir omurga görevi gören sinyal verisi ağına geçerler. Sayısal iletiş imde bağlantı bu ağ üzerinden gerçekleştirilir. Uzak uçta ise bir PC ya da bir PSTN telefonu olabilir.

IP network de ağ gecikmelerinin yanı sıra bir de paket şebekesinin oluşturduğu gecikme söz konusu. Çünkü paketler değişken gecikme süreleriyle ve düzensiz olarak(gönderilen sıradan farklı olarak) hedeflerine ulaşabilirler. Bu nedenle tekrara sıralama(resequencing),paket şebekelerinin oluşturduğu gecikmeyi dengeleme(dejitering) ve paket kayıplarının önlenmesi gerekmektedir.

IP networkün sağladığı en önemli iki avantaj :

1) Sabit bağlantı kurulumu gerektirmez, bu durum özellikle küçük boyutlu bilgi dolaşımlarında oldukça yaralıdır. Yani ağ; çok yüksekten çok düşüğe, oturuma uyum sağlayacak şekilde, değişken bant geniş likleri kullanabilir.

2) Kullanıcı eş zamanlı birden fazla oturum açabilir, aynı anda bir dosyayı indirirken ya da web'de sörf yaparken bir yandan da telefon konuşması yapabilir

PSTN olarak isimlendirilen bildiğimiz klasik telefon ağında analog ses sinyalleri ve işaretleşme olarak da CCSS(Common Chanel Signaling System) kullanılmaktadır. Internet tarafı ise IP tabanlı bir network olup sayısal veri protokolü kullanılmaktadır. Kullanılan veri ve protokollerin farklı olması dolayısı ile PSTN ile internet ağı arasında gateway kullanılmaktadır. Gateway PSTN networkünden aldığı ses ve CCSS bilgilerini dönüş türmekte ve PSTN şebekesine göndermektedir. Bu esnada gerekli olan bilgiler (hedef IP gibi) internet tarafında bulunan veri tabanlarının(gatekeeper)yardımıyla sağlanmaktadır.

1.11.2. VoIP'in Çeşitleri

Şimdiye kadar ses hizmetleri PSTN ya da ISDN gibi devre anahtarlamalı şebekeler tarafından sağlanmaktadır. Devre anahtarlamalı şebekeler bir çağrı süresince kullanıcılara tahsis edilmiş bir sondan sona bağlantı sağlar. Ancak IP şebekelerde ses çağrı yapıldığı zaman veri hareketlerine dönüştürülür ve e-maile benzer şekilde internet ya da özel şebekeler üzerindeki herhangi bir olası yol üzerinden dağıtılır. Paketler alıcı tarafında tekrar toplanır. Son kullanıcılar çağrıları bir genişbant, şebekeye bağlı bir bilgisayar ya da telefon vasıtasıyla başlatır ve alırsa çağrılar yazılım uygulamaları da kullanan diğer geniş bant abonelere yönlendirilebilir. Sistemin devre anahtarlamalı şebekelerden daha etkin olduğu düşünülmektedir.

VoIP hizmetlerinin çeşitli şekilleri bulunmaktadır. VoIP'i sınıflandırmanın bir yolu şebekeye bağlı uç birim yapılandırmalarına göredir.

Telefondan Telefona: Geleneksel telefonlar, telefon sinyallerini IP'ye çeviren ya da tam tersi yönlendiriciler vasıtasıyla bir IP şebekesine bağlanabilirler. Bu çeşit kullanım bir bilgisayar ile birlikte kullanım ihtiyacını ortadan kaldırmaktadır.

Bilgisayardan Bilgisayara: İki bilgisayar içine uygun VoIP iletişim yazılımı kurulduğu sürece kullanıcılar bilgisayarları vasıtasıyla VoIP kullanabilirler. Her iki kullanıcının herhangi bir bağlantı kurulmadan önce çevrimiçi durumda olması gerekir. Bu çeşit kullanım daha çok kamusal internet üzerinden gerçekleştirilir. Bazı özel tüketici teçhizatları (geleneksel telefonlar için adaptörler dâhil) bu manada VoIP hizmetlerini sınıflandırma amacıyla geleneksel telefondan ziyade bir bilgisayara daha çok benzemektedir.

Telefondan Bilgisayara: Geleneksel telefonlar internet üzerinden bir çağrı gerçekleştirmek için bilgisayar ihtiyacını ortadan kaldıran ağ geçitleri (gateway) vasıtasıyla bir IP şebekesine bağlandığında kullanıcılarına aynı zamanda IP şebekesine bağ lı olan bilgisayar kullanıcıları ile görüşme imkânı sağlamaktadır. Ağ geçidi PSTN'den aldığı ses trafiğini sıkıştırır, bunu bir IP şebekesi üzerine gönderir ve diğer yönde bu trafiği toplar ve çözer.

Mobil VoIP: Geçmişte pek çok VoIP çözümleri mobil telefon şebekeleriyle birlikte çalışmazdı. Son teknolojik yenilikler kullanıcıların ya mobil şebekeler ya da IP kullanan WLAN teknolojileri üzerinden ses çağrıları yapmalarına izin vermektedir. 2G mobil sistemleri ses hizmetlerini iletmek için temelde devre anahtarlamalı şebekeleri kullanırken, hâlihazırda bu sistemler paket anahtarlama ve IP yönlendirme üzerine inşa edilen çoklu-

ortam hizmetlerini sağlayacak yeteneklere sahip 3G (IMT-2000) sistemleri ile yer değiştirmektedir. Ana 3G standartlarından biri olan Kod Bölüşümlü Çoklu Erişim 2000 (CDMA 2000), çekirdek şebeke mimarisinde geliştirilmiş mobil IP kullanmaktadır. CDMA2000'in geliştirilmiş versiyonu olan CDMA2000 1x EV-DO bütün IP temelli ses, veri ve video iletişimlerini desteklemektedir. Bir diğer 3G standardı W-CDMA kendi çekirdek mimarisinde VoIP'i ve hem de diğer genişbant işitsel-görsel hizmetleri destekleyen IP Çoklu-Ortam Sistemlerini kapsamaktadır. Bazı ülkelerde mobil hizmetler içinde VoIP teknolojisini kullanma çabaları gözle görülür biçimde artmaktadır.

Kablosuz VoIP: Kablosuz VoIP alanında da gelişmeler sağlanmaktadır. Örneğin, ses iletişimlerini iletmek için kullanılan IP teknolojisi kablosuz LAN'lar (WLANs) ile birleştirilebilmektedir. WLAN orijinalinde veri şebekelerini genişletmek için bir vasıta olarak tasarlanmış olsa dahi, ses içinde bir alternatif olarak düşünülmektedir. Genellikle Wi-Fi telefon olarak adlandırılan Kablosuz teknolojiyi kullanan IP telefonu, son yıllarda gelişme göstermiş olmasına rağmen, pazar hala küçüktür. Örneğin VoIP sağlayıcı Vonage kullanıcılarının taşınabilir Wi-Fi telefonları ile WLAN erişim noktaları içinde telefon çağrıları başlatma ve almasını mümkün kılmaktadır. Birleşik Devletlerdeki en büyük mobil telefon hizmeti sağlayıcısı olan Verizon Wireless, mevcut hücresel şebekeyi ve frekansı kullanan yüksek kaliteli bir VoIP hizmeti sunmak için bir 1 Milyar USD değerinde bir kablosuz şebeke kurmaktadır. Kablosuz VoIP sistemlerinin gelişimi için, satıcıların bu tür hizmetleri mümkün kılan teçhizatın pil ömrü ve işlem gücünü geliştirmek için çalışmaları gerekecektir.

Son yıllarda ses hizmetine alternatif olarak "Wi-Fi üzerinden ses"i sunabilecek dual Wi-Fi/mobil el tipi cihazlar geliştirilmektedir. Örneğ in, Motorola ve Texas Instruments geçmiş yıllarda bir WLAN mobil telefon üzerinde dual mod ses iletimi üzerinde çalışmış ve bunu sağlayacak cihazın denemelerini gerçekleştirmiştir.

1.11.3. VoIP Protokolleri:

IP telefonu uygulamalarında en temel işlem sesin sıkıştırılmasıdır. Bu sıkıştırma ve çözümleme işlemini yapan cihazlara genellikle Codec (Coder-Decoder) denilmektedir.

VOIP'in temel problemleri güvenilirlik, ses kalitesi ve IP ve devre anahtarlamalı ağlar arasında kullanılan farklı standartların birbirleriyle uyumudur.

VOIP protokollerini incelerken iki farklı alandan bahsetmek gerekir:

1) Kontrol Alanı: arama sinyalleme ve arama kontrolünü kapsar ve konuşmayı hazırlamak ve bitirmek için gereklidir. Farklı organizasyonlar tarafından birçok standart sunulmuştur.

2) Veri Alanı : Görüşme sırasına VOIP paketlerinin iletimini yöneten protokolleri kapsar.Bu protokoller RTP(Real Time Transport Protocol)/ RTCP(Real Time Control Protocol)

1.11.3.1. RTP (Gerçek Zamanlı Taşıma Protokolü) :

Ses ve görüntünün İnternet üzerinden iletilmesi için kullanılan standart paket formatını ifade eder. Bu protokol Ses Video İletimi Çalışanları grubu tarafından geliştirilmiş ve ilk olarak 1996'da genel kullanıma sunulmuştur.

TCP/IP: Her ne kadar TCP/IP sıra numaralandırma ve paket kayıpların önleyici bir mekanizmaya sahip olsa da gerçek zamanlı uygulamalar için uygun bir protokol değildir.

UDP/IP: Bu mekanizma gerçek zamanlı uygulamalar için uygundur. Fakat UDP sıra numaralandırma ve zaman damgalama gibi hizmetler sağlamaz. RTP UDP'ye bu fonksiyonları eklemek için tasarlanmıştır.

1.11.3.2. RTCP(Gerçek Zamanlı İletim Protokolü) :

RTCP kontrol paketlerinin zaman zaman özel bir RTP oturumuna ilişkin paylaşımcılara iletimi için kullanılır. Bu kontrol paketleri paylaşımcılar hakkında(isimleri,genel adresleri gibi) bilgiler içerirler. RTCP paketlerinde bulunan en önemli bilgi ağ iletişiminin kalitesidir. Oturumdaki tüm paylaşımcılar birbirine RTCP paketleri gönderirler.

RTC ve RTCP'nin sunduğu hizmetler:

- Taşınan datanın türün tanımlanması (ses/görüntü)
- Sıra numaralandırma
- Zaman damgalama (timestamping)
- Taşıma denetleme

RTCP'nin temel fonksiyonu, RTP tarafından sağlanan hizmetin kalitesi hakkında geribildirimde bulunmaktır.

1.11.3.3. H.323

H.323 ITU(International Telecommunication Union) tarafından iki ya da daha fazla taraf arasında IP benzeri kalite servis desteği olmayan bir ağ üzerinde ses ya da görüntü trafiği taşımak için geliştirilen bir standarttır. Aslında 1990'da yerel ağlar üzerinde çoklu ortam konferansı için geliştirilmiş olan H320 standardından,ses iletişimi de eklenerek, adapte edilmiştir.

H.323'ün ilk versiyonu 1996'da ikinci versiyonu ise temmuz 1998 de ortaya çıkmıştır.H323 sesle beraber tüm çoklu ortam uygulamalarını da desteklemektedir.H323 ses kodlama, video kodlama,sistem kontrol, çoklama, çoklu ortam yayın senkronizasyonu ve yapısını içermektedir.

H323 'ün temel mimarisi dört farklı uç birimi tanımlar:

1) Gateway : PSTN ağları ile IP ağları arasındaki ara yüz ya da geçiş elemanları olarak çalışan modüllerdir. Bir gateway, paket anahtarlamalı bir ağ üzerindeki H323 uyumlu terminallerle devre anahtarlamalı bir ağdaki diğer H323 terminalleri veya diğer bir gateway arasında gerçek zamanlı çift yönlü trafik sağlayan bir ağda uç nokta(end point) olarak çalışır.IP ağ ile PSTN ağ arasındaki çağrı kurma ve kaldırma işlemlerini gatewayler üstlenirler.Video, ses ve veri formatları arasındaki dönüşüm de gatewayler tarafından gerçekleştirilir.

2) Gatekeeper: Terminallerin ve gatewaylerin kayıt, kabul ve statü takibinden sorumlu olan modüllerdir. Gatekeeper kaç kullanıcının bağlandığını ve konumlarını bilir.

Bir gatekeeper şu görevleri yerine getirir:

- Adres Dönüşümü: Kayıt mesajlarıyla günlenen bir tablo kullanarak bir alias adresini bir translation adresine çevirmek.
- Giriş Kontrolü: LAN erişimlerinde yetki denetimini kontrol etmek.
- Bantgenişliği Yönetimi: Bandwidth request ,Confirm ve Reject mesajları ile uç birimlerin bant genişliği istemlerini onaylamak ya da reddetmek.

- Zone Yönetimi: Gatekeeperların ve onların kayıtlı uç noktalarının toplamına "zone" adı verilir. Zone mantıksal bir yapıdır. Gatekeeper yukarıda anlattığımız tüm fonksiyonları kendi yönetimindeki zone için sağlar

3) Terminaller: Terminal bir IP networke direk bağlı istemci bir uç noktadır.Bu bir PC telefon a da IP telefon olarak düşünülebilir

4) Çok-uçlu kontrol birimi (Multi Point Control Unit) : MCU ağda ikiden fazla terminalin ya da gatewayin çoklu bir konferansa katılımlarını sağlamaya yarayan cihazlardır. MCU iki kısımdan oluşur: Bunlar Multipoint Controller (MC) (bulunması zorunludur) ve Multipoint Processor (MP) (bulunması zorunlu değildir) olarak adlandırılır. MC çağrı süreçlerine, konferansa katılacak bütün terminallerin ortak iletişim seviyelerinde bulunmalarını sağlamak için iletişim parametreleri üzerindeki uzlaşmaları (negotiation) sağlar. MP, MC' nin denetiminde medya streamlerinin işlenmesi (mixing, switching vb.) görevlerini yürütür. MP, yürütülen konferansın tipine göre tek bir media streamini ya da daha çok sayıda media streamini işleyebilir. En basit hali ile MCU tek bir MC' den oluşur.

1.11.3.4. SIP (Session Initiation Protokol) :

H323 çok yönlü ve oldukça kompleks bir protokoldür bundan dolayı çok faza emek ve masraf gerektirir. H323'ün bu karmaşık yapısına alternatif olarak SIP ortaya çıkmıştır. SIP IP telefonu uygulamaları için özelleşmiş, var olan protokollerin belirli kısımlarını alarak H323e göre daha küçük ve etkili bir protokol haline gelmiştir.

SIP bir ya da birden fazla katılımcının yer aldığı oturumları kurmak, değiştirmek ve sonlandırmak için tasarlanmış bir kontrol protokolüdür. Bu protokole göre bir çağrı başlatıldığı zaman gelen çağrı, çağrıyı başlatan tarafa servis veren bir sunucuya yönlendirilir. Çağrının yönlendirildiği sunucu çağrıyı reddedebilir ya da başka bir sunucuya ya da terminale yönlendirebilir. Çağrı bu şekilde cevap verecek bir sunucu buluncaya kadar ağda hiyerarşik olarak iletilir. SIP güvenilirliği kendisi sağlayıp TCP'nin güvenlikle ilgili normlarını kullanmaya gerek duymaz. SIP ilgili oturumda hangi codec in kullanılacağına karar vermek için Session Description Protokol olarak adlandırılan bir protokol kullanır.

SIP Bileşenleri :

1) SIP Kullanıcı Aracı (SIP User Agents) : SIP'i destekleyen uç aygıtlara SIP kullanıcı aracıları adı verilir. SIP'in temel amacı kullanıcı aracıları arasında kurulacak oturumlara olanak sağlamak. Bir kullanıcı aracı kullanıcılardan talimat ya da girdi alır ve diğer kullanıcı aracılarla oturum kurmak ya da kaldırmak için kendi tarafında aracılık yapar.

2) SIP Gateway : Bir SIP gateway farklı bir sinyal protokolü kullanan bir ağ ile Sıp ağı arasında ara yüz görevi gören bir uygulamadır.

3) SIP Sunucu (SIP Server) : SIP sunucuları SIP iteklerini kabul eden ve bunlara cevap gönderen uygulamalardır.

SIP'in sağladığı hizmetler:

- Kullanıcı yeri (user location): haberleşme için kullanılacak uç sistemin belirlenmesi.
- Arama kurulumu (Call setup): Arayan ve aranan telefonların zil çaldırması ve çağrı parametrelerinin kurulması.
- User capabilities: Kullanılacak media ortam ve media parametrelerini belirlenmesi.
- Arama karşılama: Çağrının transferi ve sonlandırılması.

2. YAPILAN ÇALIŞMALAR, BULGULAR VE TARTIŞMA

2.1. Giriş

Bu çalışmada, bilgi teknolojisi olan kablosuz IP telefondaki ve SIP özellikli cep telefonundaki ses haberleşmesinin kablosuz güvenlik protokollerindeki çalışmaları gözlemlenmiştir. Kablosuz güvenlik protokolleri olan WEP ve WPA protokollerinde her biri 5 dakika süren 800 test yapılarak ses sinyalleri incelenmiştir. İki protokolde de kablosuz IP telefon ve SIP özellikli cep telefonu ile kablolu IP telefon aranarak hem kablolu ağlardaki sesin iletimi hem de kablosuz ağlardaki sesin iletimi airmagnet ve PRTG programlarıyla ölçülmüştür.

2.2. Çalışma Sırasında Kullanılan Network Cihazları

2.2.1 IP Telefonlar

Ele alınan sistemde kullanılan kablosuz IP telefon Cisco markasının 7921g modeli olan kablosuz IP telefon ve cisco 7985 IP telefonudur.

Testlerde kullandığımız Şekil 18'de ki IP telefon bilgisayarlarınızın kullandığıyla aynı veri ağı üzerinden iş kullanımına uygun kalitede video sunar. IP telefon tek bir iş yeri için tasarlandığından, video görüşmelerini bir telefon araması kadar kolaylaştırır[24]. Video telefonu kullanarak arayanları görme avantajıyla birlikte çağrılar alınmasını ve yapılmasını, görüşmelerin bekletilmesini, görüşmelerin aktarılmasını, konferans görüşmeleri yapılmasını sağlar[24].

Şekil 18. Cisco 7985g IP Telefonu

Testlerde kullandığımız Şekil 19'da ki kablosuz IP telefon hem kolay kullanımı, hem kablosuz olması nedeniyle cazip bir ürün olarak iş çevrelerine sunulmaktadır. IEEE 802.11g frekansından ses iletişimini sağlayan kablosuz IP telefon Cisco CallManager ve Cisco Aironet ile entegre çalışmaktadır[22]. Wi-Fi sistemler mantığında çalışan bu telefon, güvenlik ve mobilite açısından akıllı hizmetler veren bir cihaz olarak nitelendirilmektedir.[25]

Şekil 19. Cisco 7921G İp Telefon[22]

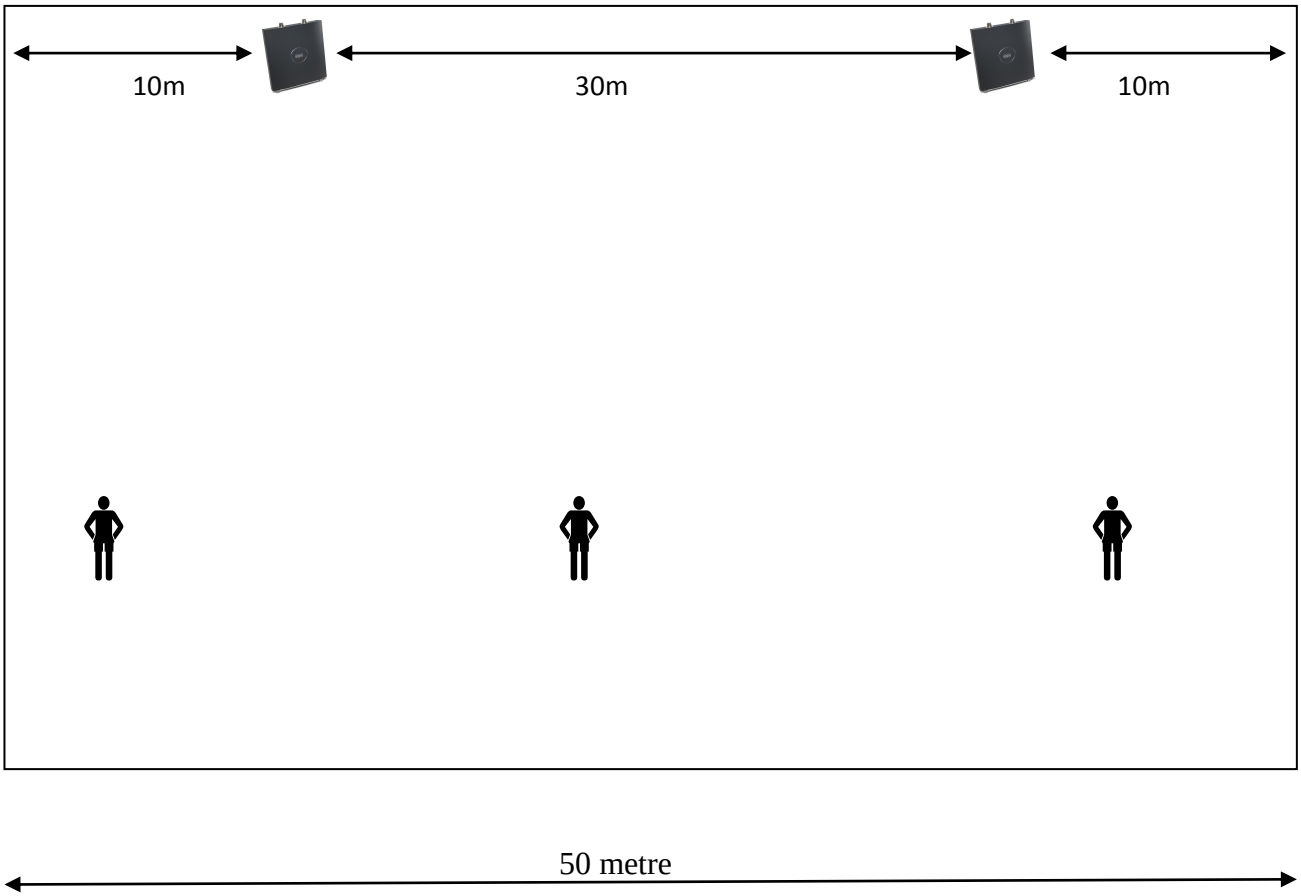
2.2.2 Access Point (Erişim Noktası)

Testlerde kullandığımız erişim noktası Cisco ’nun Şekil 20’ deki 1242 Serisi erişim noktasıdır ve 802.11i, Wi-Fi Protected Access (WPA), WPA2, ve çok sayıda Genişletilebilir Kimlik Doğrulama Protokolü (EAP) türleri destekler. WPA ve WPA2 ve WLAN güvenlik standartları ile birlikte çalışabilmeleri için Wi-Fi Alliance sertifikaları vardır. Bu sertifikalar kullanıcı tabanlı kimlik doğrulama için IEEE 802.1X, WPA şifreleme için Temporal Key Integrity Protocol(TKIP) ve WPA2 şifreleme için Gelişmiş Şifreleme Standardı (AES) destekler[23].

Şekil 20. Cisco 1242 Erişim Noktası[23]

2.3. Ses iletiminin Ölçümleri

Ölçümleri yaptığımız ortam şekil 21'de gösterildiği gibi 50 metre uzunluğundaki bir koridorda aralarında 30 metre mesafe olan 2 adet erişim noktasının montajı yapılarak gerçekleştirilmiştir.

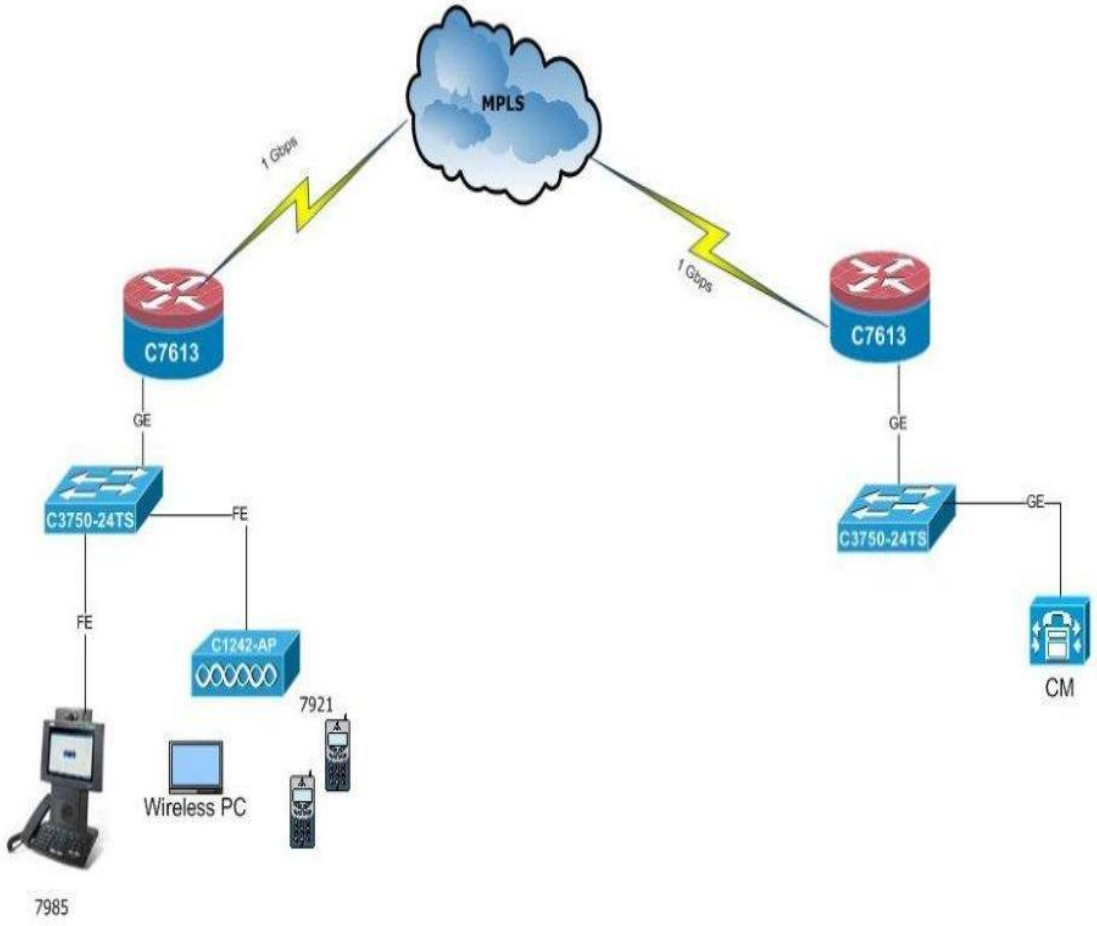


Şekil 21. Ölçümlerin Yapıldığı Ortam

2.3.1.Otonom Modda Çalışan Erişim Noktalarında Yapılan Testler

Erişim noktası otonom modda çalışırken toplamda 400 test yapılmıştır. Her test 5 dakika sürmüştür. Testler sırasında gürültünün azaltılması ve ses sinyallerinin kaliteli olması için ağ üzerinde sadece bu iki telefona özel ses vlanı oluşturuldu ve başka hiçbir cihaz bu vlana dahil edilmedi. Yine de ağ üzerinde call manager farklı bir şube de olduğu için ve bu telefonlar bu call managera register oldukları ve call manager üzerinden konuştukları için kayıplar yine çok olmuştur.

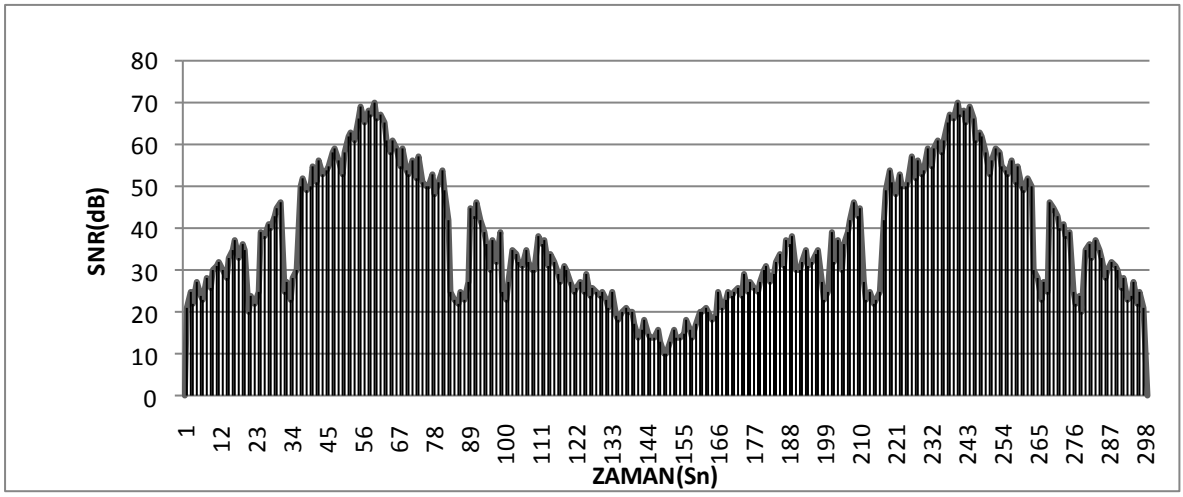
2.3.1.1. Kablosuz IP Telefonla Yapılan WEP Güvenlik Politikası Testi



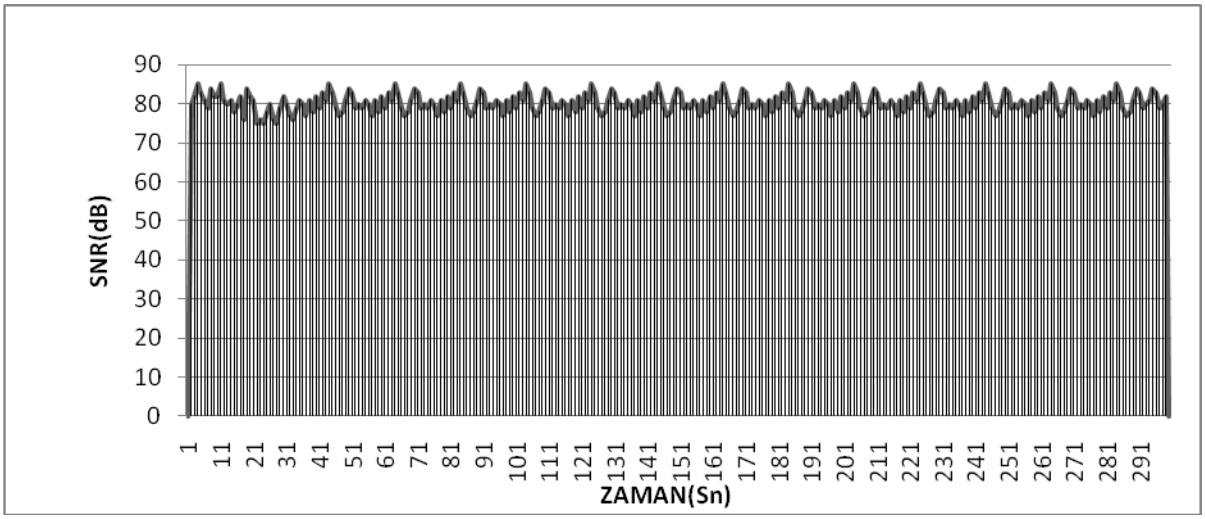
Şekil 22. Erişim noktasının otonom modda çalışması için kurulan ağ topolojisi[19].

Yukarıdaki Şekil 22'de gösterilen ağda erişim noktasının konfigürasyonu otonom modda çalışacak şekilde yapıldı ve içinde TEST adında SSID oluşturuldu. Bu SSID de önce güvenliği WEP olarak ayarlayıp 40 bitlik bir şifre oluşturduk. Kablosuz IP telefondaki ayarlar yapıldıktan sonra kablolu IP telefon arayarak hem kablosuz IP telefondaki sinyali airmagnet programıyla hem de kablolu IP telefonda ki sinyal PRTG

programı ile gözlemledik. Her biri 5 dakika süren 150 test yapıldı. Testler boyunca kablolu IP telefondan gönderilen ses hep aynı tutuldu ve ağda gürültünün az olması için sadece sesin iletimi için gereken portlar aktif edildi. Gözlemler sonucu çıkan grafikler aşağıda Şekil 23 ve 24'te gösterilmektedir.



Şekil 23. WEP protokolünde çalışan kablosuz IP telefondaki ses sinyali

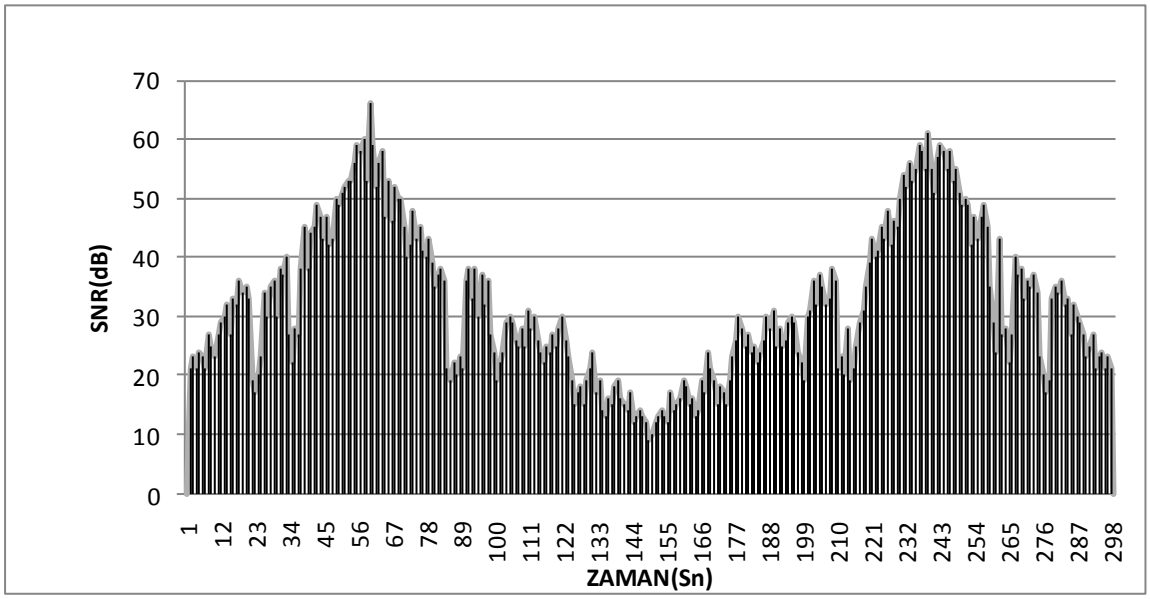


Şekil 24. Kablolu IP telefondaki ses sinyali

Şekillerde de görüldüğü gibi otonom moda çalışan erişim noktaları üzerinde çalışan kablosuz IP telefondaki ses datası iletilirken WEP güvenlik politikasında sinyallerdeki kayıplar kablolu IP telefondaki sinyallere göre daha çoktur. WEP şifrelemesinde şifreleme işlemi 40 bit olduğu için seste kayıp 128 bit şifrelemeye oranla daha azdır.

2.3.1.2. Kablosuz IP Telefonla Yapılan WPA Güvenlik Politikası Testi

Şekilde 22'de gösterilen ağda erişim noktasının konfigürasyonu otonom modda çalışacak şekilde yapıldı ve içinde TEST adında ssıd oluşturuldu. Bu ssıd güvenliği WPA olarak ayarlandı. Kablosuz IP telefondaki ayarlar yapıldıktan sonra kablolu IP telefon arayarak hem kablosuz IP telefondaki sinyali airmagnet programıyla hem de kablolu IP telefonda ki sinyal PRTG programı ile gözlemledik. Her biri 5 dakika süren 150 test yapıldı. Testler boyunca kablolu IP telefondan gönderilen ses hep aynı tutuldu ve ağda gürültünün az olması için sadece sesin iletimi için gereken portlar aktif edildi. Gözlemler sonucu çıkan Şekil 24ve 25' de gösterilmektedir.

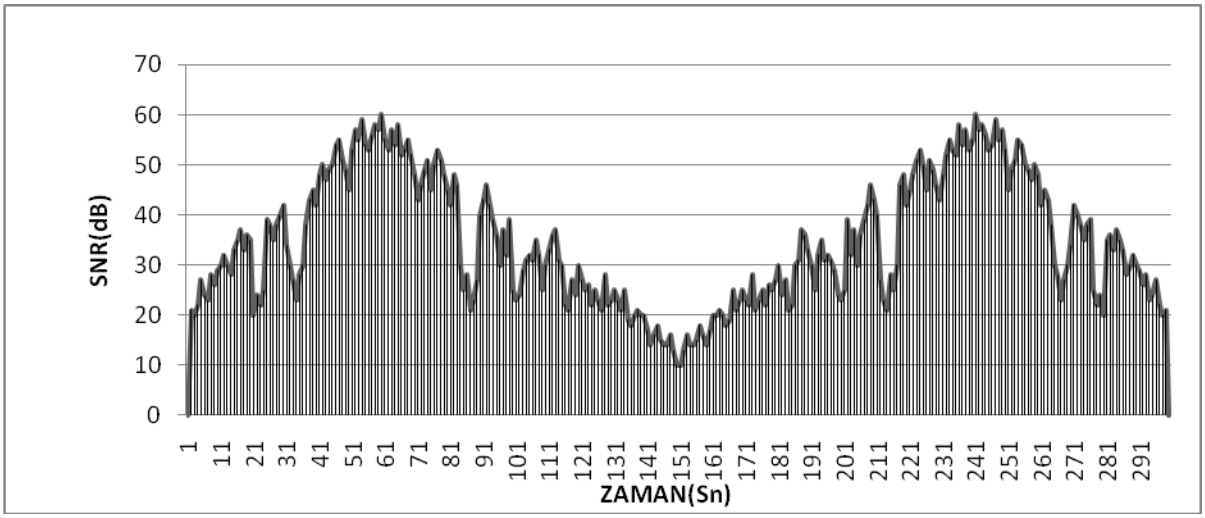


Şekil 25. WPA protokolünde çalışan kablosuz IP telefondaki ses sinyali

Şekillerde de görüldüğü gibi otonom moda çalışan erişim noktası üzerinde çalışan kablosuz IP telefondaki ses datası iletilirken WPA güvenlik politikasındaki ses sinyallerindeki kayıplar kablolu IP telefondaki ses sinyallerine göre oldukça fazladır.

2.3.1.3. SIP Özellikli Cep TelefonuylaYapılan WEP Güvenlik Politikası Testi

Yukarıdaki Şekil 22'de gösterilen ağda erişim noktasının konfigürasyonu otonom modda çalışacak şekilde yapıldı ve içinde TEST adında SSID oluşturuldu. Bu SSID de önce güvenliği WEP olarak ayarlayarak 40 bitlik bir şifre oluşturduk. SIP özellikli cep telefonundaki ayarlar yapıldıktan sonra kablolu IP telefonu arayarak hem SIP özellikli cep telefonundaki sinyali airmagnet programıyla hem de kablolu IP telefonda ki sinyal PRTG programı ile gözlemledik. Her biri 5 dakika süren 50 test yapıldı. Testler boyunca kablolu IP telefondan gönderilen ses hep aynı tutuldu ve ağda gürültünün az olması için sadece sesin iletimi için gereken portlar aktif edildi. Gözlemler sonucu çıkan grafikler aşağıda Şekil 24 ve Şekil 26'da gösterilmektedir.

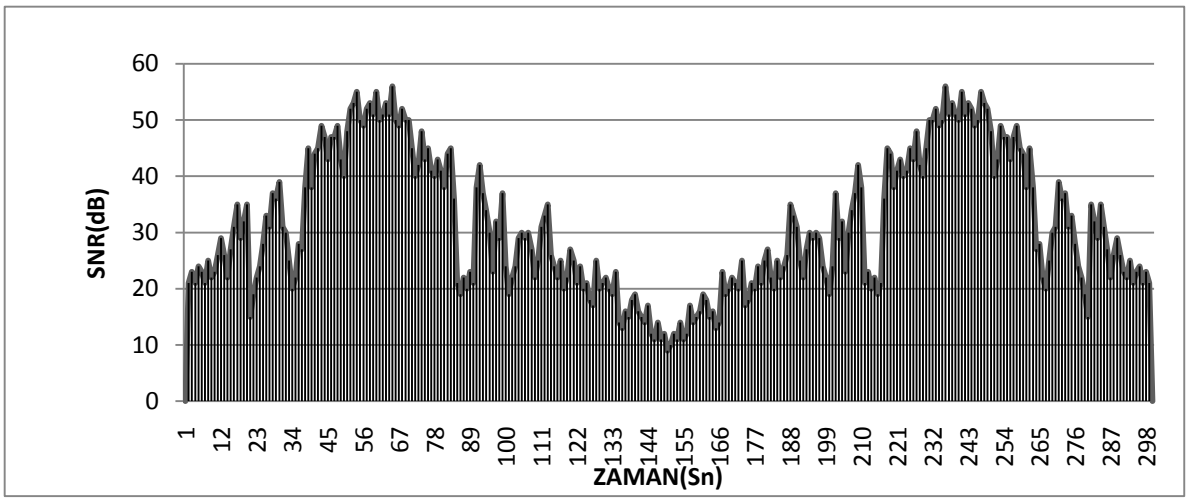


Şekil 26. WEP protokolünde çalışan SIP özellikli cep telefonundaki ses sinyali

Şekillerde de görüldüğü gibi otonom moda çalışan erişim noktası üzerinde çalışan SIP özellikli cep telefonundaki ses datası iletilirken WEP güvenlik politikasında sinyaller kablolu IP telefondaki sinyallere göre kayıplar fazladır. WEP şifrelemesinde şifreleme işlemi 40 bit olduğu için seste kayıp 128 bit şifrelemeye oranla daha azdır.

2.3.1.4. SIP Özellikli Cep Telefonuyla Yapılan WPA Güvenlik Politikası Testi

Şekilde 21'de gösterilen ağda erişim noktasının konfigürasyonu otonom modda çalışacak şekilde yapıldı ve içinde TEST adında SSID oluşturuldu. Bu SSID güvenliği WPA olarak ayarlandı. Kablosuz IP telefondaki ayarlar yapıldıktan sonra kablolu IP telefon arayarak hem SIP özellikli cep telefonundaki sinyali airmagnet programıyla hem de kablolu IP telefonda ki sinyal PRTG programı ile gözlemledik. Her biri 5 dakika süren 50 test yapıldı. Testler boyunca kablolu IP telefondan gönderilen ses hep aynı tutuldu ve ağda gürültünün az olması için sadece sesin iletimi için gereken portlar aktif edildi. Gözlemler sonucu çıkan grafikler Şekil 24 ve Şekil 27'de gösterilmektedir.

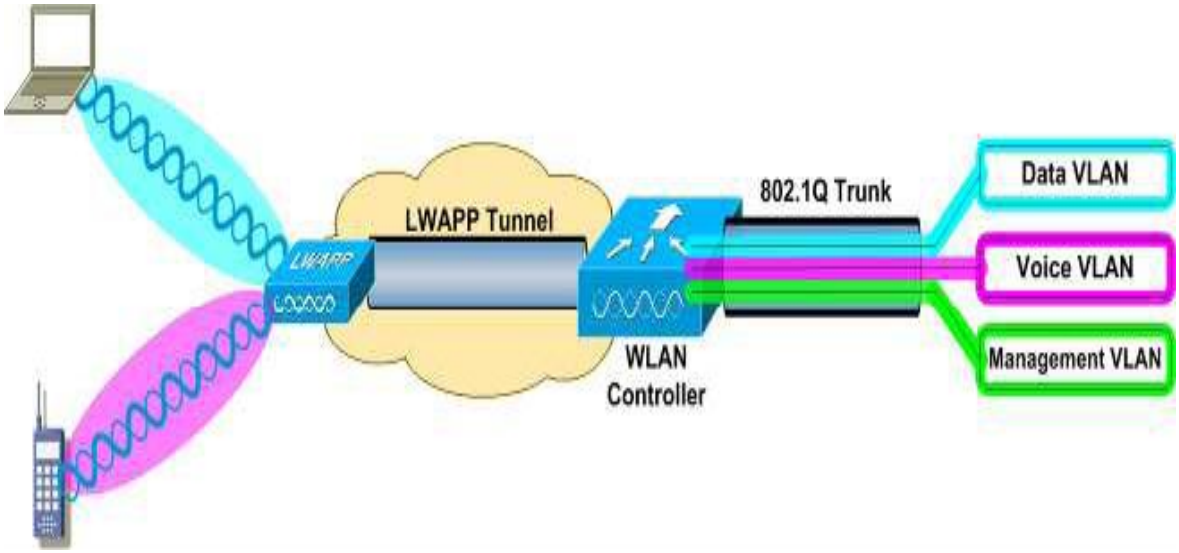


Şekil 27. WPA protokolünde çalışan SIP özellikli cep telefonundaki ses sinyali

Şekillerde de görüldüğü gibi otonom modda çalışan erişim noktası üzerinde çalışan SIP özellikli cep telefonundaki ses datası iletilirken WPA güvenlik politikasında sinyallerdeki kayıplar kablolu IP telefondaki sinyallere göre daha çoktur. 128 bitlik bir şifreleme olduğu için WEP güvenlik politikasındaki ses sinyallerine göre de WPA güvenlik politikasındaki ses sinyalleri daha zayıftır.

2.3.2. Hafif Erişim Noktası Protokolü (LWAPP) ile Çalışan Erişim Noktalarında Yapılan Testler

Hafif Erişim Noktası Protokolü (Light Weight Access Point Protocol, LWAPP) denetleyebilir bir protokoldür. Bu, izleme ve geniş bir ağdaki sorunlarını giderme süresini azaltır. Sistem ağ yöneticilerin ağı daha yakından analiz etmelerini de sağlamaktadır. Erişim cihazları ile denetleyici cihazlar arasında kullanılır. Denetim ve veri trafigini taşır. Bu taşıma sırasında denetim verilerini AES-CCM şifreler.

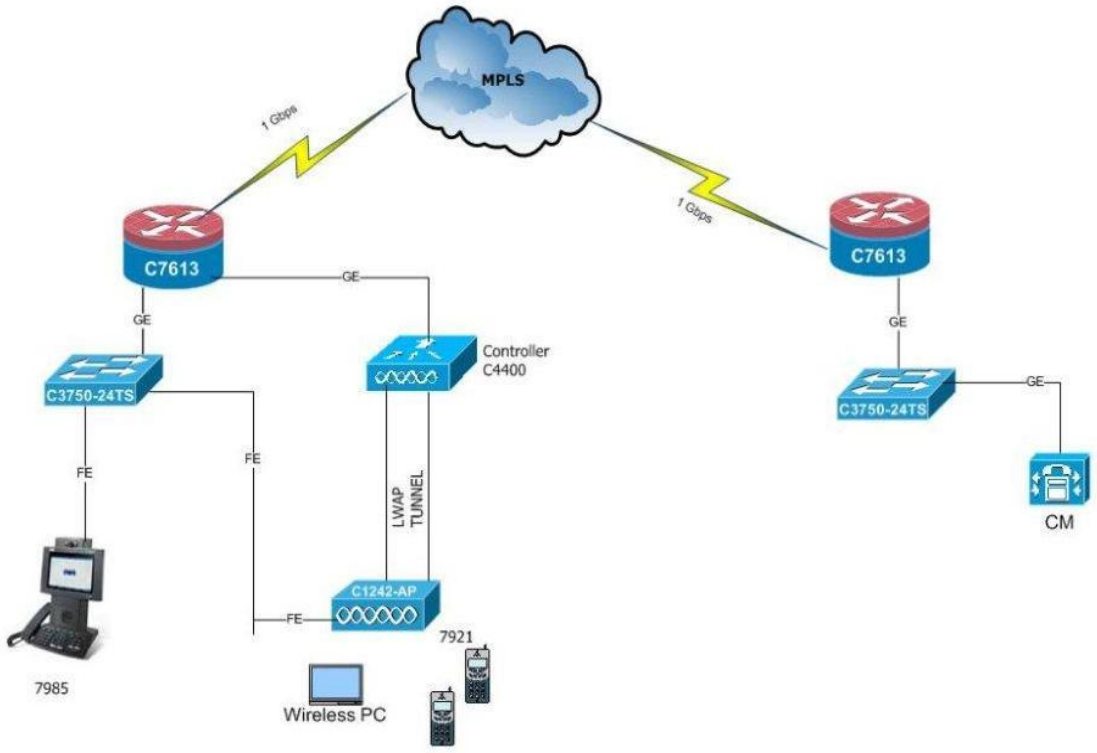


Şekil 28. LWAPP çalışma şekli[20].

Şekil 28'de de görüldüğü gibi LWAPP protokolünde erişim noktası ile denetleyici controller arasında özel bir LWAPP tüneli açılıyor ve veriler ile denetim verileri bu tünelden geçiyor.

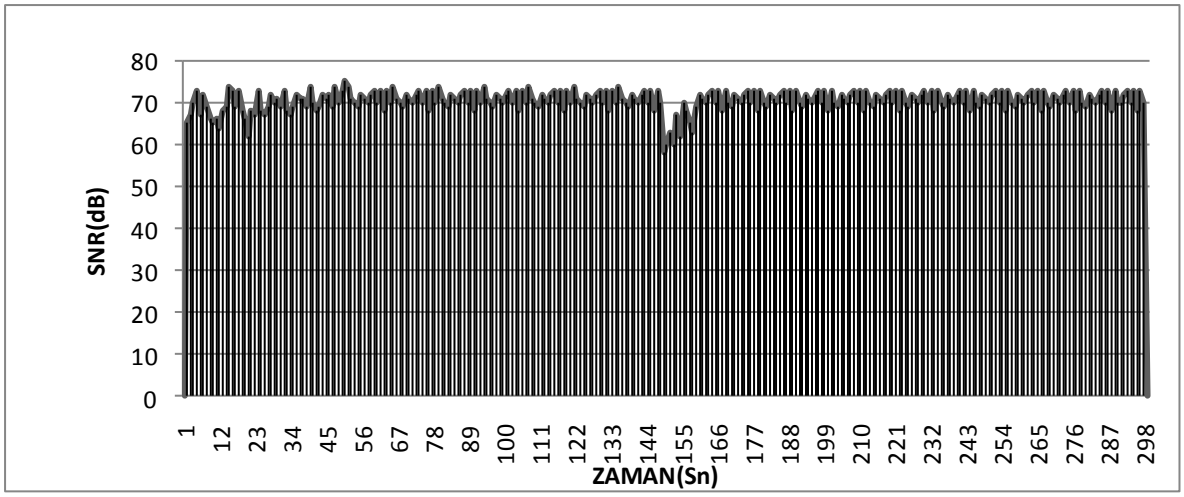
Erişim noktası LWAPP modda çalışırken toplamda 400 test yapılmıştır. Her test 5 dakika sürmüştür. Testler sırasında gürültünün azaltılması ve ses sinyallerinin kaliteli olması için ağ üzerinde sadece bu iki telefona özel ses vlanı oluşturuldu ve başka hiçbir cihaz bu vlana dahil edilmedi. Yine de ağ üzerinde call manager farklı bir şube de olduğu için ve bu telefonlar bu call managera register oldukları ve call manager üzerinden konuştukları için kayıplar olmuştur.

2.3.2.1. Kablosuz IP Telefonla Yapılan WEP Güvenlik Politikası Testi

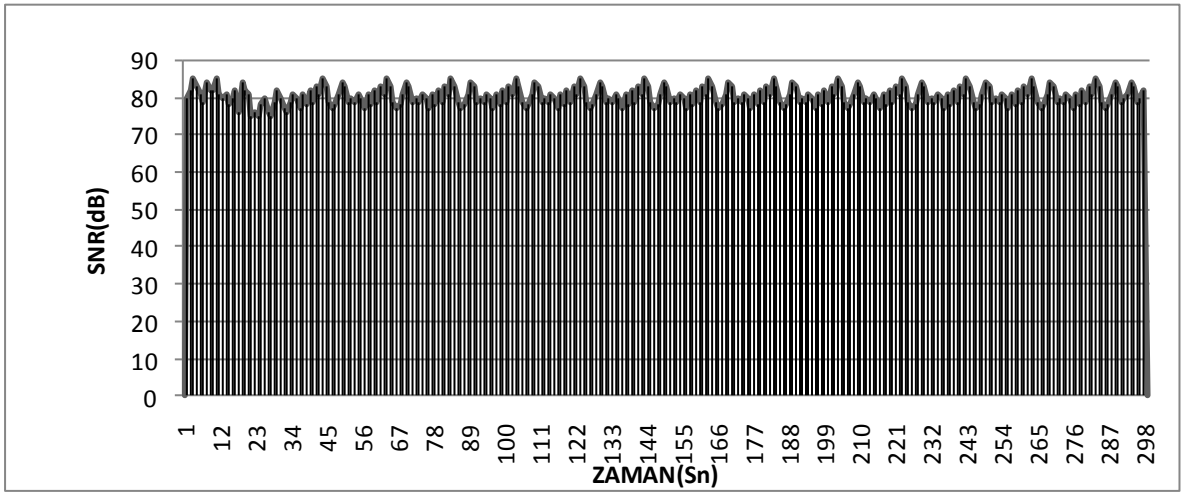


Şekil 29: Erişim Noktasının LWAPP modda çalışması için kurulan ağ topolojisi[19].

Yukarıdaki şekilde 29'da gösterilen ağda erişim noktasının konfigürasyonu LWAPP modda çalışacak şekilde yapıldı. Yani LWAPP çalışacak şekilde yazılımı güncellendi ve wireless lan controller(WLC) a register oldu. WLC üzerinde TEST adında SSID oluşturuldu ve bu SSID erişim noktası üzerinden yayınlandı. Denetleyici yani WLC üzerinde bu ssıd de önce güvenliği WEP olarak ayarlayıp 40 bitlik bir şifre oluşturduk. Kablosuz IP telefondaki ayarlar yapıldıktan sonra kablolu IP telefon arayarak hem kablosuz IP telefondaki sinyali airmagnet programıyla hem de kablolu IP telefonda ki sinyal PRTG programı ile gözlemledik. Her biri 5 dakika süren 150 test yapıldı. Testler boyunca kablolu IP telefondan gönderilen ses hep aynı tutuldu ve ağda gürültünün az olması için sadece sesin iletimi için gereken portlar aktif edildi. Gözlemler sonucu çıkan grafikler aşağıda Şekil 30 ve Şekil 31'de gösterilmektedir.



Şekil 30. WEP protokolünde çalışan kablosuz IP telefondaki ses sinyali

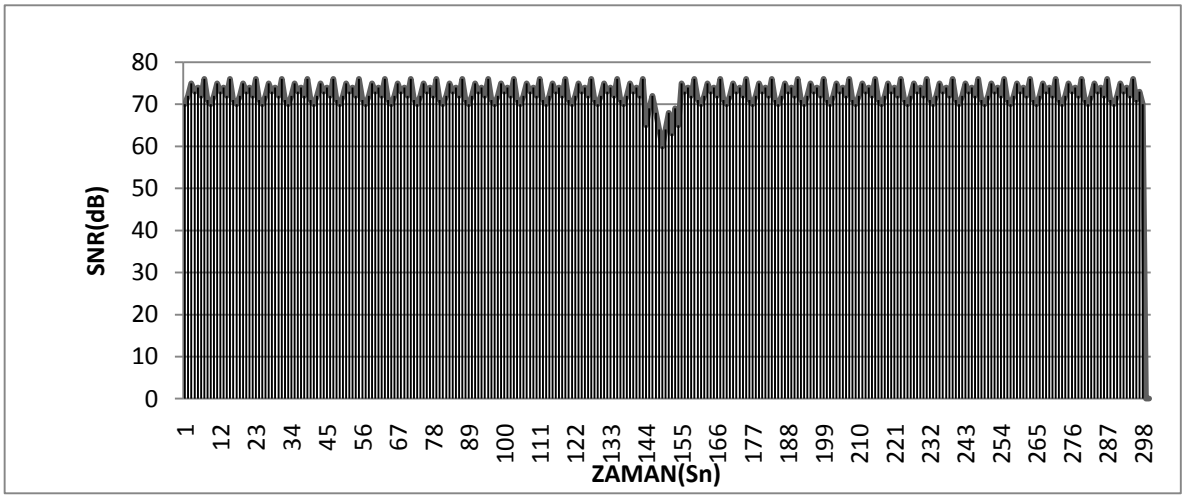


Şekil 31. Kablolu IP telefondaki ses sinyali

Şekillerde de görüldüğü gibi LWAPP modda çalışan erişim noktası üzerinde çalışan kablosuz IP telefondaki ses datası iletilirken güvenlik politikasındaki ses sinyallerindeki kayıplar kablolu IP telefondaki sinyallere göre fazla değildir. WEP şifrelemesinde şifreleme işlemi 40 bit olduğu için seste kayıp 128 bit şifrelemeye oranla daha azdır.

2.3.2.2. Kablosuz IP Telefonla Yapılan WPA Güvenlik Politikası Testi

Şekil 28'de erişim noktası LWAPP modda çalışacak şekilde konfigürasyonu yapıldı. Yani LWAPP çalışacak şekilde yazılımı güncellendi ve wireless lan controller(WLC) a register oldu. WLC üzerinde TEST adında SSID oluşturuldu ve bu SSID erişim noktası üzerinden yayınlandı. Denetleyici yani WLC üzerinde bu SSIDde güvenlik WPA olarak ayarlandı. Kablosuz IP telefondaki ayarlar yapıldıktan sonra kablolu IP telefon arayarak hem kablosuz IP telefondaki sinyali *airmagnet* programıyla hem de kablolu IP telefonda ki sinyal *PRTG* programı ile gözlemledik. Her biri 5 dakika süren 150 test yapıldı. Testler boyunca kablolu IP telefondan gönderilen ses hep aynı tutuldu ve ağda gürültünün az olması için sadece sesin iletimi için gereken portlar aktif edildi. Gözlemler sonucu çıkan grafikler şekil31 ve şekil32'de gösterilmektedir.

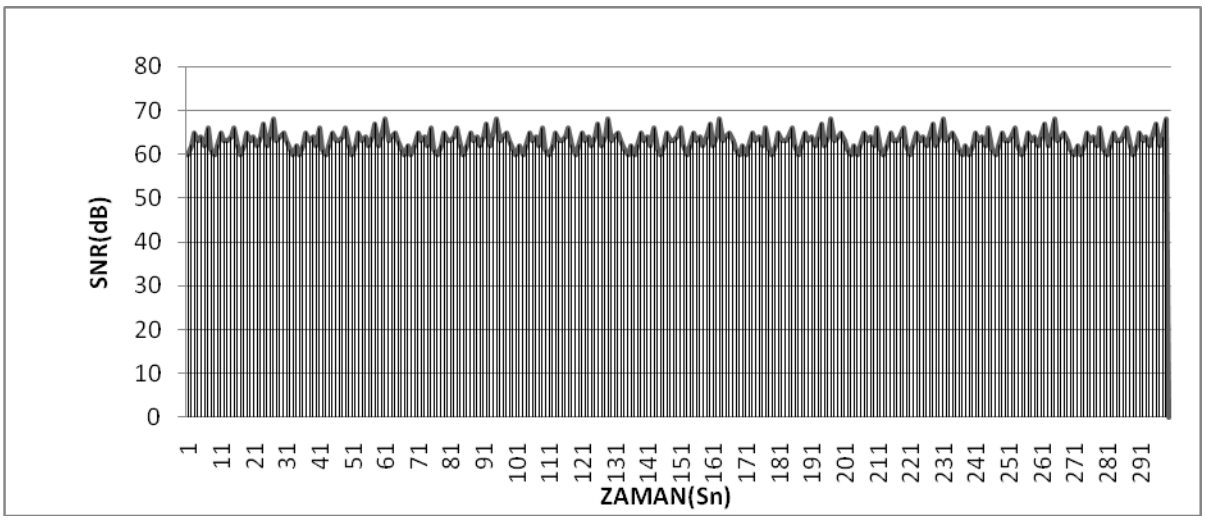


Şekil 32. WPA protokolünde çalışan kablosuz IP telefondaki ses sinyali

Şekillerde de görüldüğü gibi LWAPP modda çalışan erişim noktası üzerinde çalışan kablosuz IP telefondaki ses datası iletilirken WPA güvenlik politikasındaki ses sinyallerindeki kayıplar kablolu IP telefondaki sinyallere göre fazla değildir.

2.3.2.3. SIP Özellikli Cep Telefonuyla Yapılan WEP Güvenlik Politikası Testi

Şekilde 29'da gösterilen ağda erişim noktasının konfigürasyonu LWAPP modda çalışacak şekilde yapıldı. Yani LWAPP çalışacak şekilde yazılımı güncellendi ve wireless lan controller(WLC) a register oldu. WLC üzerinde TEST adında SSID oluşturuldu ve bu SSID erişim noktası üzerinden yayınlandı. Denetleyici yani WLC üzerinde bu ssıd de önce güvenliği WEP olarak ayarlayıp 40 bitlik bir şifre oluşturduk. SIP özellikli cep telefonundaki ayarlar yapıldıktan sonra kablolu IP telefon arayarak hem SIP özellikli cep telefonundaki sinyali airmagnet programıyla hem de kablolu IP telefonda ki sinyal PRTG programı ile gözlemledik. Her biri 5 dakika süren 50 test yapıldı. Testler boyunca kablolu IP telefondan gönderilen ses hep aynı tutuldu ve ağda gürültünün az olması için sadece sesin iletimi için gereken portlar aktif edildi. Gözlemler sonucu çıkan grafikler aşağıda Şekil 31 ve Şekil 33'de gösterilmektedir.

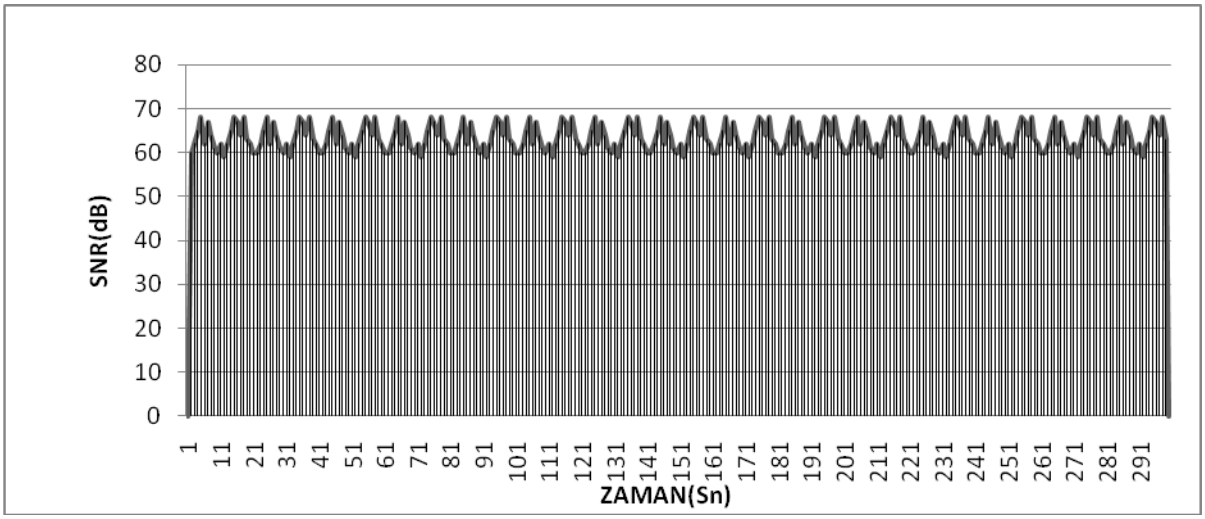


Şekil 33. WEP protokolünde çalışan SIP özellikli cep telefonundaki ses sinyali

Şekillerde de görüldüğü gibi LWAPP modda çalışan erişim noktası üzerinde çalışan SIP özellikli cep telefonundaki ses datası iletilirken WEP güvenlik politikasındaki ses sinyallerindeki kayıplar kablolu IP telefondaki sinyallere göre fazla değildir.

2.3.2.4. SIP Özellikli Cep Telefonuyla Yapılan WPA Güvenlik Politikası Testi

Şekil 29'da erişim noktası LWAPP modda çalışacak şekilde konfigürasyonu yapıldı. Yani LWAPP çalışacak şekilde yazılımı güncellendi ve wireless lan controller(WLC) a register oldu. WLC üzerinde TEST adında SSID oluşturuldu ve bu SSID erişim noktası üzerinden yayınlandı. Denetleyici yani WLC üzerinde bu SSID de güvenlik WPA olarak ayarlandı. SIP özellikli cep telefonundaki ayarlar yapıldıktan sonra kablolu IP telefon arayarak hem SIP özellikli cep telefonundaki sinyali *airmagnet* programıyla hem de kablolu IP telefonda ki sinyal *PRTG* programı ile gözlemledik. Her biri 5 dakika süren 50 test yapıldı. Testler boyunca kablolu IP telefondan gönderilen ses hep aynı tutuldu ve ağda gürültünün az olması için sadece sesin iletimi için gereken portlar aktif edildi. Gözlemler sonucu çıkan grafikler Şekil 31 ve Şekil 34'de gösterilmektedir.

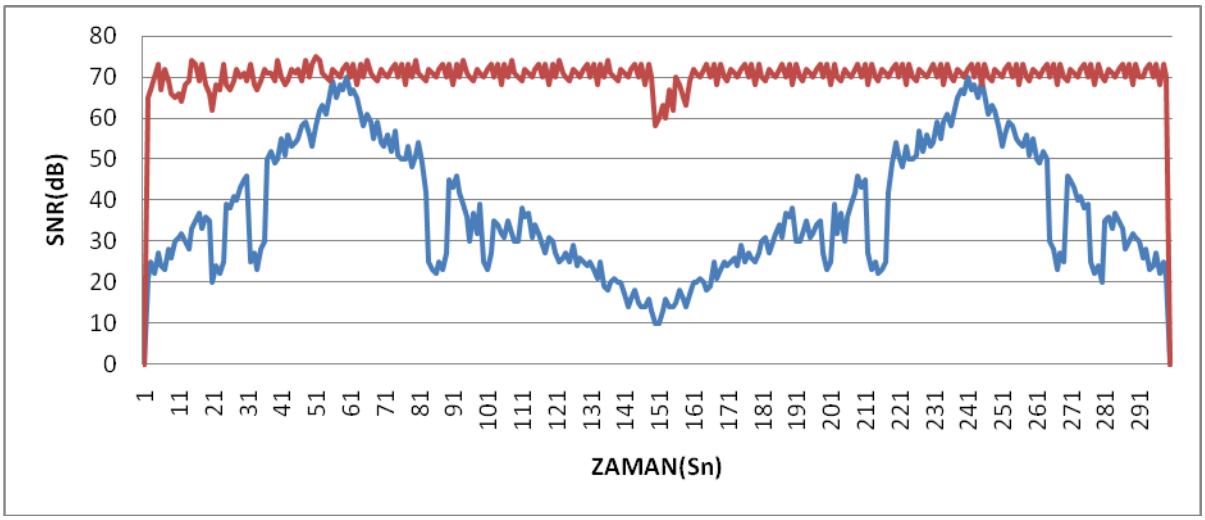


Şekil 34. WPA protokolünde çalışan SIP özellikli cep telefonundaki ses sinyali

Şekillerde de görüldüğü gibi LWAPP modda çalışan erişim noktası üzerinde çalışan SIP özellikli cep telefonundaki ses datası iletilirken WPA güvenlik politikasındaki ses sinyallerindeki kayıplar kablolu IP telefondaki sinyallere göre fazla değildir.

2.3.3. Sistem Performansı Değerlendirme

Grafiklerde de gördüğümüz gibi erişim noktası otonom modda çalıştığı zaman oluşturulan TEST SSID sinde WEP şifrelemesi kullanılması veri kaybının azlığı nedeniyle tercih edilebilir ama güvenli olmaz. Erişim noktası LWAPP modunda çalışırken WEP ve WPA güvenlik protokollerinin ikisini de incelediğimiz zaman kayıplar fazla olmamaktadır.



Şekil 35. Otonom-LWAPP Modların Performans Analizi

Şekil 35'de kablosuz ağda erişim noktaları WPA güvenlik protokolü ile çalıştırıldığı zaman ki performansları görünmektedir. Şekildeki kırmızı renkteki ses sinyali erişim noktaları LWAPP modda çalışırken gözlemlenen ses sinyalidir. Mavi renkteki ses sinyali ise erişim noktaları otonom modda çalışırken gözlemlenen ses sinyalidir.

Şekil 35'e baktığımız zaman Kablosuz IP telefon LWAPP modda çalışan erişim noktası üzerinden çalışırken ses sinyallerinde(kırmızı renk) 5-10dB civarında kayıp varken otonom moda çalışan erişim noktası üzerinden çalışırken ses sinyallerinde(mavi renk) ortalama 35-45dB civarında kayıplar olmaktadır.

Konuşmanın ortasında erişim noktaları otonom modda çalışırken kablosuz IP telefondaki ses sinyalleri 10dBye kadar düşüyor ve görüşme kesiliyor. Bu arada telefon bir erişim noktasından kopup diğerine bağlanmaya çalışıyor. Bunun nedeni otonom modda çalışan erişim noktası üzerinden çalışan kablosuz IP telefondaki ses sinyallerini hem erişim noktalarının birbirinden bağımsız çalışması hem de etraftaki 2.4GHz de çalışan diğer cihazların girişim yapmasından dolayı oldukça fazla olmasıdır.

LWAPP moda çalışan erişim noktalarında ise bu kayıplar azdır. Çünkü; her iki erişim noktasının LWAPP moda çalışırken aslında bir cihaz gibi davranmaları ve etraftaki cihazlarla girişim olmaması için çalıştıkları kanalları otomatik değiştirmelerinden dolayı kayıplar azdır ve telefon görüşmesi kesilmemektedir.

Kablosuz IP telefonla konuşurken eğer karşı tarafta konuştuğumuz cihaz da kriptolama özelliği yoksa yani her iki tarafta da kriptolama özelliği yoksa konuşulanların güvenliği sadece kablosuz ağdaki güvenlik önlemleriyle alınabilir. Yapılan testler sonucun da ağda ne kadar çok önlem alırsak alalım kablosuz ağın olduğu kısımdan yine konuşmalar dinlenebiliyor. Bu dinlemeyi önlemek için WPA şifrelemeyi kullanmak daha önemlidir.

Hem güvenli hem de az kayıplı ses trafiğini iletmek için erişim noktasını LWAPP moda çalıştırmalıyız ve WPA güvenliğini uygulamalıyız.

Erişim noktası LWAPP modunda çalışırken SIP özellikli cep telefonlarıyla da görüşmeler oldukça net yapılabilmektedir. Marka uyumsuzluğu olmasına rağmen kayıplar azdır.

3. SONUÇLAR

Günümüzde telefon sistemleri IP tabanlı sistemlere dönmektedir. Sadece masamızda ki telefonlar değil aynı zamanda mobilite açısından da DECT telefonlar yerine kablosuz IP telefonlar kullanılmaktadır.

Yapılan haberleşmenin başkalarınca dinlenmemesi, kayıt ve kopya edilmemesi için alınacak güvenlik önlemleri büyük önem arz etmektedir. Eğer haberleşmenin yapıldığı her iki telefonun da kriptolama ya da şifreleme özelliği yoksa haberleşmenin güvenliği sadece kablosuz ağlarda uygulanan güvenlik politikaları ile sağlanmaktadır. Günümüzde ev telefonlarında ve cep telefonlarında kriptolama özelliği olmadığı için kablosuz IP telefondan ev telefonu ya da cep telefonu arandığında kablosuz ağlardaki güvenlik politikaları çok büyük önem teşkil etmektedir.

Kablosuz ağlardaki güvenlik politikalarından ilk geliştirilen WEP politikasının çok fazla güvenlik açığı olmasından dolayı WPA güvenlik politikası geliştirildi. WPA geliştirildiği zaman WEP politikasıyla uyumlu çalışan cihazlarda ek donanım ve yazılım ihtiyacı ortaya çıkmıştır. Bununla birlikte yeni donanım ve yazılım sistemin güvenliğini büyük oranda artırmış, haberleşmenin dinlenmesini nerdeyse imkansız hale getirmiştir.

Bu çalışmada, kablosuz ağ üzerinden yapılan ses haberleşmesinin kalitesi araştırılmış, kablosuz ağlarda en güvenli ve en kaliteli ses haberleşmesinin nasıl yapılacağı tespit edilmiştir.

Yapılan testlerde erişim noktalarının birinci nesil protokol ile çalışırken birbirlerinden bağımsız olarak çalıştığı ve erişim noktasından uzaklaşıldıkça data kayıplarının arttığı görülmüştür. Dolayısı ile haberleşme kalitesi çok düşük olmaktadır.

Deneysel çalışmalarda da görüldüğü gibi WEP ve WPA nın her ikisininin de ikinci nesil protokol ile çalıştırıldığında (erişim noktalarında LWAPP protokolü çalıştırıldığında) data kayıpları yok denecek kadar azalmaktadır. Haberleşmenin güvenli yapılabilmesi için kablosuz IP telefonların WPA güvenlik şifrelemesi ile çalıştırılmasının daha uygun ve güvenli olduğu sonucuna varılmıştır. Bu gerek ağ gerekse haberleşme güvenliği açısından daha doğru bir işlem olarak ortaya çıkmaktadır.

WPA, 128 bitlik şifrlemesi ve diğer önlemlerine karşılık, fiziksel yapı ve taşınabilir cihazlarda uygulanan yazılım kısıtlamalarından dolayı kullanımı zor bir sistemdir. Dolayısı ile henüz güvenlik problemini istenilen düzeyde çözümleyememektedir.

4. ÖNERİLER

1. Bu çalışmada, test edilecek birimin tabi olduğu standarda göre ölçümleri yapılmıştır. Sonuçların doğru bir fikir verebilmesi açısından test ölçümlerinin defalarca yapılması önemlidir.
2. Kablosuz ve ya kablolu ağlarda sesin kalitesini korumak için ses vlanı oluşturulmalı ve sadece ip telefonlar bu vlana alınmalıdır.
3. Kablosuz ağlarda güvenlik protokollerinin yanı sıra kablosuz ip telefon için oluşturulan ssid gizli tutulursa kablosuz ağın güvenliği bir basamak daha artırılmış olur.
4. Büyük şirketler ya da çalışanı fazla olan kuruluşlar kuracakları kablosuz ağlarda mümkün olduğunca erişim noktalarını lwapp modda çalışacak şekilde kurarlarsa bu hem yönetim hem de güvenlik açısından oldukça kolaylık sağlayacaktır.
5. Kurulacak olan kablosuz ağlarda wep güvenlik protokolü yerine wpa güvenlik protokolü seçilirse bu kablosuz ağın güvenliğini artıracaktır.
6. İp telefon sistemlerine geçilmek istendiğinde kurulacak olan Call Manager'ın eğer kampus tarzı bir yerleşkeyse kampüse değilse tüm sistemlerin bulunduğu lokasyona kurulması ses iletiminde verinin kalitesinin azalmamasına yardımcı olacaktır.
7. Tüm voip uygulamaları büyük band genişliği istediği için kurulacak ağlarda hızın düşük tutulmaması çok önemlidir. Bir ip telefon 2Mb band genişliğini meşgul edecektir.

5. KAYNAKLAR

1. WLANA Organization and Education, What is a Wireless LAN? [online], http://www.wlana.org/learn/educate1.htm 05/05/2010.

2. DUNNE, D., What is a wireless LAN? [online] http:// www.cnn.com /TECH /ptech/what.is.WLAN.idg/index.html 04/09/2010.

3. Stallings, W., "Data & Computer Communications 6th Ed.", 250-300, Prentice Hall, 2000.

4. Tanenbaum, A. S., "Computer Networks, Fourth Edition", Prentice Hall, Chapter 4, 2003.

5. Öztürk, E., WLAN Kablosuz Yerel Alan Agları (Wireless Local Area Networks) Teknolojisinin İncelenmesi, Mevcut Düzenlerin Degerlendirilmesi ve Ülkemize Yönelik Düzenleme Önerisi (Uzmanlık Tezi). Telekomünikasyon Kurumu, Ankara. 2004.

6. Baykal, N., Bilgisayar Aglarına Giris, Bölüm 12.Bilgisayar Agları.1.Baskı.SAS Bilisim, Ankara. 2001.

7. WONG, J., Performance Investigation of Secure 802.11 Wireless LANs Raising the Security Bar to Which Level?, Thesis (MS), Master of Commerce in Accountancy, Finance, and Information Systems, University of Canterbury. 2003,

8. WEBOPEDIA, Webopedia Online Dictionary for Computer and Internet Terms [online], http://www.webopedia.com/index.html, 02/08/2010.

9. NETWORKWORLD.COM, Network World Fusion [online], http:// www.nwfusion.com/index.html, 25/01/2010.

10. BORISOV, N., GOLDBERG, I., WAGNER, D., 2001, (In)Security of the WEP Algortihm, [online], http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html, 18/05/2010.

11. WONG, S., The evoluation of wireless security in 802.11 networks: WEP, WPA and 802.11 standarts , GSEC Practical v1.4b, 2003.

12. HANNINEN, T., *WiFi Security*, Department of Computer Science University of Helsinki, Finland, 2003.

13. National Institute of Standards and Technology, , *Advanced Encryption Standard* [online], http://csrc.nist.gov/CryptoToolkit/aes/, 2001.

14. Hammand, J., Kessler, B., Rivero, J., Skinner, C. ve Sweeney, T., Wireless Hotspot Deployment Guide, Mobile Platfroms Group-WVP: 32-49. 2003.

15. Çölkesen R. ve Örencik B., "Bilgisayar Haberleşmesi ve Ağ Teknolojileri", Papatya Yayıncılık, İstanbul, 2000.

16. Forouzan B., "Data Communications and Networking", Mc-Graw Hill, New York, 2006.

17. S. Oktuğ, "İTÜ Bilgisayar Mühendisliği Bölümü Bilgisayar Haberleşmesi Ders Notları", İTÜ, 2004.

18. Önder, M., Karataş, H., CCNA INTRO Sınav Sertifikasyon Rehberi, Sistem Yayıncılık,İstanbul-506, 2006.

19. Anonim, TT-Intranet Eğitim Notları, TÜRK TELEKOM A.Ş., Ankara, 2010.

20. Anonim, Oryantasyon Veri İletişimi Temel Bilgileri, TÜRK TELEKOM A.Ş. Ankara, 2007.

21. Stallings W., "Wireless Communications and Networks", Prentice Hall, New Jersey, 2004.

22. http://www.dibekiletisim.com.tr/download/Cisco-IP-Phone-7921G-Brosur-EN.pdf, 14/12/2009.

23. http://www.cisco.com/en/US/products/ps6521/index.html,23/03/2010.

24. http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/phones/ps379/ps6564/roduct_data_sheet0900aecd8030e546.html,27/11/2009

25. http://www.cisco.com/en/US/products/ps7071/index.html, 12/07/2010

26. Kula, G. Ç., 'Mosquito Dizi Şifreleme Algoritmasının VHDL ile yazılımı ve FPGA Üzerine Gerçeklenmesi", İstanbul Teknik Üniversitesi, Elektrik-Elektronik Fakültesi, Türkiye.2006.

27. FIBS 197, Advanced Encryption Standard. National Institute of Standarts and Technology (NIST). 2001.

28. Doğan, A. H., "AES Algoritmasının FPGA Üzerinde Düşük Güçlü Tasarımı'', Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Türkiye, 2006

29. Ferguson, N., Schneier B., Practical Cryptography. Wiley Pulishing, Inc., Indianapolis, Indiana, 2003.

ÖZGEÇMİŞ

Soner KADAKOĞLU 1982 yılında Ankara'da doğdu. İlk öğrenimini Kent Koop İlköğretim Okulunda, Orta öğrenimini Samanyolu Koleji ve Lise öğrenimini Ankara Gazi Anadolu Lisesi'nde yaptı. 2001 yılında Karadeniz Teknik Üniversitesi, Mühendislik Mimarlık Fakültesi, Elektrik-Elektronik Mühendisliği Bölümü'nde Lisans Programı'na başladı ve 2006 yılında bu bölümden mezun oldu. Aynı yıl Karadeniz Teknik Üniversitesi, Fen Bilimleri Enstitüsü Elektronik Mühendisliği Ana Bilim Dalı'nda Yüksek Lisans Programı'na başladı. TÜRK TELEKOM A.Ş.'de BT Ağ Yönetimi Müdürlüğünde Mühendis olarak çalışmaktadır. Yabancı dil olarak iyi seviyede İngilizce bilmektedir.