T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

802.11 KABLOSUZ YEREL ALAN AĞLARINDA GÜVENLİK SORUNU

YÜKSEK LİSANS TEZİ

Ahmet Sertol KÖKSAL

Enstitü Anabilim Dalı : ELEKTRONİK VE BİLGİSAYAR EĞİTİMİ

Tez Danışmanı : Yrd. Doç. Dr. Hayrettin EVİRGEN

Mayıs 2007

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

802.11 KABLOSUZ YEREL ALAN AĞLARINDA GÜVENLİK SORUNU

YÜKSEK LİSANS TEZİ

Ahmet Sertol KÖKSAL

Enstitü Anabilim Dalı : ELEKTRONİK VE BİLGİSAYAR EĞİTİMİ

Bu tez 09/05/2007 tarihinde aşağıdaki jüri tarafından oybirliği ile kabul edilmiştir.

Yrd. Doç. Dr. Hayrettin EVİRGEN	Prof. Dr. Abdullah FERİKOĞLU	Yrd. Doç. Dr. İbrahim ÖZÇELİK
Jüri Başkanı	**Üye**	**Üye**

TEŞEKKÜR

Tezimin her aşamasında her türlü desteği veren danışman hocam Sayın Yrd. Doç. Dr. Hayrettin EVİRGEN'e, önerilerinden dolayı tezime katkıda bulunan Sayın Yrd. Doç. Dr. Turan ÇAKIR'a, Linux sistemleri hakkında teknik desteğini esirgemeyen Sakarya Üniversitesi Bilgi İşlem Dairesi çalışanlarından Şadan AKINCI, Tarık DEMİRGEN ve Kadir ASLAN beylere ve araştırmalarımda yardımlarını esirgemeyen Sayın Seyit Rıza KUŞCU arkadaşıma teşekkür ederim.

Ahmet Sertol KÖKSAL

İÇİNDEKİLER

SİMGELER VE KISALTMALAR LİSTESİ

AES	:	Advanced Encryption Standard
AP	:	Access Point
ARP	:	Address Resolution Protocol
BSS	:	Basic Service Set
CBC	:	Cipher Block Chaining
CCMP	:	Counter Mode – CBC MAC Protocol
CDMA	:	Code Division Multiple Access
CHAP	:	Challenge Handshake Authentication Protocol
CSMA/CA	:	Carrier Sense Multiple Access/Collision Avoidance
CSMA/CD	:	Carrier Sense Multiple Access with Collision Detection
DDoS	:	Distributed Denial of Service
DFS	:	Dynamic Frequency Selection
DoS	:	Denial of Service
DSS	:	Distribution Service Set
DSSS	:	Direct Sequence Spread Spectrum
EAP	:	The Extensible Authentication Protocol
EAPOL	:	The Extensible Authentication Protocol Over LAN
EAP-TLS	:	EAP-Transport Layer Security
ESS	:	Extended Service Set
ETSI	:	European Telecommunications Standards Institute
FDMA	:	Frequency Division Multiple Access
FHSS	:	Frenquency Hopping Spread Spectrum
HiperLAN	:	High Performance Radio LAN
HMACSHA1	:	Hashed Message Authentication Code-Secure Hash Algorithm 1
IBSS	:	Independent Basic Service Set
ICV	:	Integrity Check Value
IEEE	:	Institute of Electrical and Electronic Engineers

IETF	:	Internet Engineering Task Force
IPSec	:	Internet Protocol Security
ISM	:	Industrial, Scientific, Medical
IV	:	Initialization Vector
LAN	:	Local Area Network
LLC	:	Logical Link Control
MAC	:	Medium Access Control
MAN	:	Metropolitan Area Network
MIC	:	Message Integrity Code
MIMO	:	Multiple Input Multiple Output
MITM	:	Man In The Middle
MITMOT	:	Mac and Mimo Technologies for More Throughput
MMAC	:	Multimedia Mobile Access Communications Systems
MPDU	:	Media Access Control Protocol Data Unit
MS-CHAPv2	:	Microsoft Challenge Handshake Protocol version 2
MSDU	:	Media Access Control Service Data Unit
NIC	:	Network Interface Card
NIST	:	National Institute of Standards and Technology
OFDM	:	Orthogonal Frequency Division Multiplexing
PAN	:	Personal Area Network
PEAP	:	Protected EAP
PHY	:	Physical
PLCP	:	Physical Layer Convergence Procedure
PMD	:	Physical Medium Dependent
PMK	:	Pairwise Master Key
PPP	:	Point-to Point Protocol
PRNG	:	PseudoRandom Number Generator
PSK	:	Preshared Key
PTK	:	Pairwise Transient Key
QAM	:	Quadrature Amplitude Modulation
QoS	:	Quality of Service
RADIUS	:	Remote Authentication and Dial-In User Service

RF	:	Radio Frequency
RSN	:	Robust Security Network
SSID	:	Service Set Identification
STA	:	Station
TDMA	:	Time Division Multiple Access
TGnSync	:	Task Group N Synchronization
TKIP	:	Temporal Key Integrity Protocol
TPC	:	Transmission Power Control
TSC	:	TKIP Sequence Counter
VPN	:	Virtual Private Network
WAN	:	Wide Area Network
WECA	:	Wireless Ethernet Compatibility Alliance
WEP	:	Wired Equivalent Privacy
Wi-Fi	:	Wireless Fidelity
WLAN	:	Wireless Local Area Network
WMAN	:	Wireless Metropolitan Area Network
WPA	:	Wi-Fi Protected Access
WPAN	:	Wireless Personal Area Network
WWAN	:	Wireless Wide Area Network
WWise	:	Worldwide Spectrum Efficiency

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

ÖZET

Anahtar kelimeler: Kablosuz ağlar, IEEE 802.11, WEP, WPA, WPA2, 802.1x, kablosuz ağ güvenliği.

Bu tezin amacı, güvenli bir kablosuz ağ oluşturmak için kullanılan yöntemleri incelemektir. Kablolu ağlar, kablosuz ağ standartları ve güvenlik mekanizmaları hakkında bilgiler içerir.

Bu kapsamda farklı kablosuz ağ güvenlik standartlarına ilişkin iki uygulama yapılmış ve çoğu kablosuz ağ yapılandırmalarının güvenli olmadığı tespit edilmiştir. Geliştirilen son güvenlik teknolojileri ile güvenli bir kablosuz ağ kurulabileceği gözlenmiştir. Tam anlamıyla güvenli bir kablosuz ağ oluşturmak için, en son güvenlik teknolojilerinin kullanılması gerektiği sonucuna varılmıştır.

SECURITY ISSUE OF 802.11 WIRELESS LOCAL AREA NETWORKS

SUMMARY

Keywords: Wireless networks, IEEE 802.11, WEP, WPA, WPA2, 802.1x, Wireless security.

The aim of this thesis is investigating methods for a secure wireless network setup. This thesis includes information about wired networks, wireless network standards and security mechanisms.

According to this thesis two case studies are done about different wireless network standards and as a result it shows that most common wireless network configurations are not secure. Newly developed security technologies help us to configure secure wireless networks. As a result newly developed security technologies are needed to configure a full secure wireless network.

BÖLÜM 1. GİRİŞ

Kablosuz iletişim kullanıcıların iletişim esnasında mekândan bağımsız olabildikleri, hareket özgürlüğüne sahip oldukları bir iletişim şeklidir. Bu hareketlilik insanların ihtiyaçları doğrultusunda gelişim göstermektedir. Bugün hayatımızın artık her anında bilgiye her yerden, cep telefonları, cep bilgisayarları ve dizüstü bilgisayarlar aracılığıyla ulaşmamız mümkündür.

Kablosuz iletişim teknolojisi, en basit tanımıyla, noktadan noktaya veya bir ağ yapısı şeklinde bağlantı sağlayan, bir teknolojidir. Bu açıdan bakıldığında, kablosuz iletişim teknolojisi, günümüzde yaygın olarak kullanılan kablolu veya fiber optik iletişim yapılarıyla benzerlik göstermektedir. Kablosuz iletişim teknolojisini diğerlerinden ayıran nokta ise; iletim ortamı olarak havayı kullanmasıdır. Bu tez çalışmasında kablosuz yerel alan ağları incelenmiştir. Kablosuz yerel alan ağları, günümüzde en yaygın şekliyle WLAN (Wireless Local Area Network) olarak adlandırılmaktadır.

WLAN sistemleri iş adamları, yöneticiler, çalışanlar, küçük işletmeler, orta ölçekli işletmeler ve bireysel kullanıcılar gibi büyük bir kesime, internet ve üyesi oldukları kurumsal ağa kablosuz bağlanma imkânı sağlamaktadır. Kablolu LAN'ların tüm özelliklerine sahip olan WLAN sistemleri bu ağların devamı ya da alternatifi olarak kullanılmaktadırlar. Kurumsal ve kişisel kullanımın dışında restoranlar, otobüs terminalleri, oteller, büyük alışveriş merkezleri, tren istasyonları, hava alanları cadde ve sokaklar gibi kamuya açık alanlarda erişim alanları vasıtasıyla verilen kablosuz internet hizmetinin de hızla artmakta olduğu görülmektedir.

WLAN sistemleri, endüstri kuruluşları veya bu kuruluşların katkıları ile oluşturulan organizasyonlar tarafından yürütülen çalışmalar sonucu lisans gerektirmeyen frekans bantlarında geliştirilmektedir. Bu çalışmalar WLAN sistemlerinin çok hızlı bir şekilde yaygınlaşmasını sağlamaktadır. Ancak, tüm bu olumlu gelişmelerin yanı sıra

WLAN sistemlerinin iletişim ortamı olarak havayı kullanmasından kaynaklanan bazı kısıtlamalar ve güvenlik problemleri de vardır. Bu tez çalışmasında, WLAN için geliştirilen güvenlik mekanizmaları, karşılaşılan problemler, ağa yapılan saldırılar, kablosuz ağ güvenliğinin sağlanması için geliştirilen çözüm yöntemleri incelenmiştir.

Konunun daha iyi anlaşılması için, ikinci bölümde; gerek benzerlikleri gerekse birlikte çalışmaları açısından kablolu ağların yapıları, topolojileri, güvenlik mekanizmaları ve ağ bağlantı cihazları hakkında kısa bilgi verilmiştir. Üçüncü bölümde ise; WLAN modülasyon ve erişim teknikleri, topolojileri, avantaj - dezavantajları ve kullanılan standartlar incelenmiştir.

Dördüncü bölümde; 802.11 standardını kullanan kablosuz yerel alan ağlarındaki güvenlik mekanizmaları incelenmiş; güvenlik açıkları, sistemin zayıflıkları ve ağa yapılan saldırıların neler olduğu araştırılmıştır. Daha sonra, kablosuz bir ağ üzerinde farklı güvenlik mekanizmaları yapılandırılıp, bu ağa saldırılar gerçekleştirmek suretiyle bir uygulama yapılmıştır. Diğer bir uygulamada ise Sakarya İli'ninin belli bölgelerinden alınan kablosuz ağ örneklerinin özellikleri güvenlik açısından incelenmiş ve bu ağların güvenilirlikleri analiz edilmiştir.

Bu tez çalışmasının amacı; bireysel kullanımdan en kapsamlı ve gelişmiş kurumsal kullanıma kadar, güvenli bir kablosuz yerel alan ağı oluşturmak için izlenmesi gereken politikaları ve olası saldırılara karşı en güvenilir yöntemleri belirlemektir.

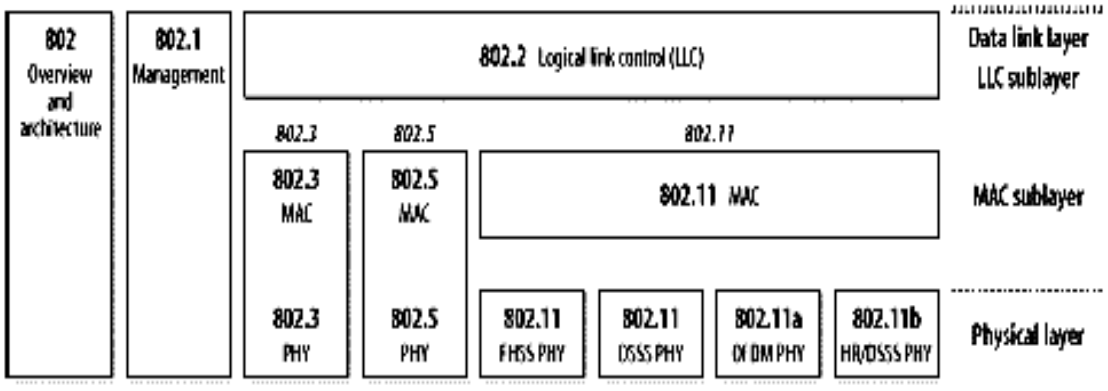
BÖLÜM 2. 802.11 AĞLARININ TANITIMI

2.1. Giriş

802.11 kablosuz ağları tıpkı Ethernet teknolojisinde olduğu gibi işlemleri gerçekleştirebilecek şekilde tasarlanmıştır. İlk bakışta 802.11 Ethernet ile benzerdir. Ancak Ethernet altyapısı ile 802.11 ağlarını işletmek mümkün değildir.

Kablosuz 802.11 ağları için Ethernet altyapısına yeni eklentiler yapılması gerekmektedir. Bu şekilde kablosuz dünyada geleneksel Ethernet teknolojisi ile bir uyum sağlanabilmektedir. Ayrıca 802.11 ağlarına kablolu ve kablosuz her iki ortamda uyum içinde çalışabilmesi için eklentiler de yapılmıştır.

802.11, yerel alan ağları (LAN) teknolojileri için standart tanımlamalarını yapan IEEE 802 ailesinin bir üyesidir. Şekil 2.1'de 802 ailesinin farklı bileşenleri arasındaki ilişki ve onların OSI referans modelindeki yerleri gösterilmektedir.



Şekil 2.1. 802 ailesi ve OSI referans modeli ile ilişkisi [26]

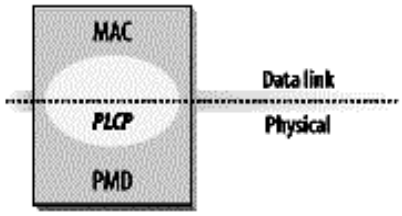
IEEE 802 tanımlamaları OSI referans modelinin iki katmanında yer almaktadır. Bu katmanlar OSI referans modelinin en altında yer alan fiziksel katman ve veri bağlantı katmanıdır. Bütün 802 ağları bir MAC (Medium Access Control) ve PHY (Physical)

bileşenine sahiptir. MAC, ortama erişim ve verinin gönderilmesi kurallarını koyar. Gönderim ve alım ayrıntıları ise PHY tarafından işletilir.

802 serisinin özel tanımlamaları ikinci bir numara tarafından yapılmaktadır. Örneğin 802.3, Ethernet ile ilişkili CSMA/CD (Carrier Sense Multiple Access with Collision Detection), 802.5 Token Ring tanımlamasını yapar. Diğer tanımlamalar da 802 protokollerinin diğer parçalarını ifade eder. 802.2 özel tanımı, alt katmanlı LAN teknolojileri tarafından kullanılabilen LLC (Logical Link Control) ortak bağ katmanını tanımlar. 802 ağları için yönetim özellikleri 802.1 tarafından belirtilmektedir. 802.1 yayınları arasında köprüleme için (802.1d) ve sanal LAN için (802.1q) tanımlamaları bulunmaktadır.

802.11, 802.2/LLC özelliklerini kullanabilen farklı bir bağ katmanıdır. Temel 802.11 tanımlaması MAC ve iki fiziksel katman içerir: birincisi frekans atlamalı geniş spektrum (FHSS) fiziksel katmanı, ikincisi düz sıralı geniş spektrum (DSSS) bağ katmanıdır. 802.11'deki sonraki düzenlemeler fiziksel katmanlara yeni eklentiler yapmıştır. 802.11b yüksek hızlı bir DSSS (high-rate DSSS) tanımlar. 1999'da 802.11b tabanlı ürünler oldukça sıklıkla kullanılmaya başlamıştır. 802.11a, frekans atlamalı çoğullama (OFDM) tabanlı bir fiziksel katman tanımlar.

802.11 için, 802.2'nin sadece farklı bir bağ katmanıdır denebilir. 802.11 gezgin ağ erişimine izin verir. Bu amaçla, MAC içinde ek özellikler birleştirilmiştir. Sonuç olarak 802.11 MAC diğer IEEE 802 MAC tanımlamalarına göre daha karmaşık bir yapıda görünebilir.



Şekil 2.2. PHY bileşenleri [26]

Radyo dalgalarının kullanımı karmaşık PHY'de olduğu gibi bir fiziksel katmana gereksinim duyar. 802.11 PHY'yi iki bileşene ayırır: PLCP (Physical Layer Convergence Procedure) MAC çerçevelerini ortam üzerinde adresler; PMD (Physical Medium Dependent) sistemi bu çerçeveleri iletir. PLCP Şekil 2.2'de görüldüğü gibi MAC ve fiziksel katmanın sınırındadır. 802.11'de PLCP, çerçevenin havada iletildiğine dair yeni bir alan ekler [26].

2.6. Kablosuz İletişim Ağları

Kablosuz iletişim ağları iki veya daha fazla bilgisayar veya sayısal cihazın birbirleriyle kablosuz veri iletişimi sağlamalarıyla oluşan yapıdır. Bu ağlar; özel amaçlı, eğitim amaçlı, ulusal veya halka açık olarak kurulabilirler. Kablolu iletişim teknolojilerine kıyasla birçok üstünlüğü bulunan kablosuz iletişim teknolojileri 1990'lı yıllarda büyük gelişmelere sahne olmuştur [1].

Kablosuz iletişim teknolojisi, günümüzde yaygın olarak kullanılan kablolu iletişim yapılarıyla benzerlik göstermektedir. Kablosuz iletişim teknolojisini diğerlerinden ayıran nokta ise; iletim ortamı olarak havayı kullanmasıdır. Metal kablolar, elektrik akımını iletirken kablosuz iletim sistemleri belli frekanstan elektromanyetik dalga iletmektedir. Kablosuz ağların, gönderim ortamı olarak havayı kullanmasından dolayı, kendine özgü kısıtların yanında, güvenlik sorunu da bulunmaktadır [2,3].

Bu ağların büyüklüklerine göre sınıflandırılması WLAN (Wireless Local Area Network) sistemlerinin daha iyi incelenebilmesi açısından tercih edilmektedir.

2.7. Büyüklüklerine Göre Kablosuz Ağlar

Kablosuz iletişim ağlarını hizmet verdikleri fiziksel alanlara göre gruplandırmak mümkündür. Ancak teknolojideki hızlı gelişme ve sistemlerdeki yakınsama bu gruplandırmada kesin çizgilerin çizilmesini zorlaştırmaktadır. Genel bir yaklaşıma göre kablosuz iletişim ağları, 4 sınıf altında toplanabilir. Bunlar; Kablosuz Geniş Alan Ağları (WWAN – Wireless Wide Area Network), Kablosuz Metropol Alan Ağları (WMAN – Wireless Metropolitan Area Network), Kablosuz Yerel Alan

Ağları (WLAN – Wireless Local Area Network) ve Kablosuz Kişisel Alan Ağları (WPAN – Wireless Personal Area Network) olarak sıralanabilir [4]. Tablo 1.1'de kablosuz ağların standartları, hızları, mesafeleri ve uygulamaları gösterilmiştir.

2.7.1. WWAN

Bir ülke ya da dünya çapında yüzlerce veya binlerce kilometre mesafeler arasında iletişimi sağlayan ağlara Geniş Alan Ağları (WAN) denilmektedir. WAN'larda genellikle kiralık hatlar veya telefon hatları kullanılmaktadır. Bu tür ağlarda kablo yerine uydu veya telsiz iletişimi kullanılması durumunda Kablosuz Geniş Alan Ağları (WWAN) olarak isimlendirilmektedir. WWAN'larda trafik yükünün büyük kısmı ses iletişimi ile ilgilidir. Ancak son yıllarda yoğun olarak veri iletişimi ve internet erişimi talepleri yaşanmaktadır. WWAN uygulamalarına örnek olarak GSM, GPRS, CDMA ve 3G sistemleri sayılabilir [4].

2.7.2. WMAN

Bir şehri kapsayacak şekilde yapılandırılmış iletişim ağlarına veya birbirinden uzak yerlerdeki yerel bilgisayar ağlarının birbirleri ile bağlanmasıyla oluşturulan ağlara Metropol Alan Ağları (MAN) denilmektedir. MAN'larda da WAN'larda olduğu gibi genellikle kiralık hatlar veya telefon hatları kullanılmaktadır. Bu tür ağlarda kablo yerine uydu veya RF iletişimi teknolojileri kullanılması durumunda Kablosuz Metropol Alan Ağları (WMAN) olarak isimlendirilmektedir. WMAN'lar çok sayıda şubesi bulunan kurum ve büyük şirketler ile dağınık yerleşime sahip üniversiteler gibi yapılarda yaygın olarak kullanılmaktadır. IEEE 802.16 standardı WMAN için geliştirilmektedir [5].

2.7.3. WLAN

Yerel alan ağları (LAN) bir bina, okul, hastane, kampüs gibi sınırlı bir coğrafi alanda kurulan ve çok sayıda kişisel bilgisayarın yer aldığı ağlardır. LAN'lar, kamu kurum ve kuruluşlarında, şirketlerde, üniversitelerde, konferans salonlarında ve benzeri pek çok yerde kullanılmaktadır. LAN'larda bilgisayarlar ve ağ içerisindeki diğer cihazlar

arasında iletişimi sağlamak üzere kablo yerine RF (Radio Frequency) veya kızılötesi teknolojisi kullanılması durumunda, Kablosuz Yerel Alan Ağları (WLAN) olarak adlandırılmaktadır. WLAN sistemleri; kullanıcılarına kablosuz geniş bant internet erişimi, sunucu üzerindeki uygulamalara ulaşım, aynı ağa bağlı kullanıcılar arasında elektronik posta hizmeti ve dosya paylaşımı gibi çeşitli imkânlar sağlamaktadır. Ayrıca kablosuz bir sistem olması nedeniyle cadde, sokak, park, bahçe ve benzeri açık alanlarda WLAN sistemleri başarılı bir şekilde kullanılmaktadır. Ancak yerel kullanım amacıyla geliştirilmiş olduklarından WLAN sistemlerinin mesafesi 25-100 metre civarındadır. Dünyada yaygın olarak kullanılan 2 tür WLAN teknolojisi mevcuttur. Bunlardan birisi Amerika tabanlı IEEE 802.11x ve diğeri ise Avrupa tabanlı HiperLAN sistemleridir [1].

2.7.4. WPAN

WPAN'lar yakın mesafedeki elektronik cihazları kablosuz olarak birbirine bağlayan ağlardır. Bu tür sistemler diğer ağlara kıyasla daha düşük veri hızına ve daha kısa iletişim mesafesine sahiptirler. WPAN'ların hızları 1 Mbps ve menzilleri 10 metre civarındadır. WPAN'ların en yaygın uygulamaları Bluetooth ve HomeRF'dir.

Tablo 2.1. Kablosuz İletişim Teknolojileri

	WPAN	**WLAN**	**WMAN**	**WWAN**
Standart	Bluetooth HomeRF	IEEE 802.11 HiperLAN	IEEE 802.16 HiperMAN	GSM, GPRS, CDMA ve 3G
Hız	< 1 Mbps	11 – 54 Mbps	11 – 100 Mbps	10 – 384 Kbps
Mesafe	Kısa	Orta	Orta – Uzun	Uzun
Uygulama	Cihazlar arası bağlantı Piconet	Cihazdan cihaza Ağ kurulumu	Kablo yerine Son kullanıcı erişimi	Mobil Telefon Mobil Veri

BÖLÜM 3. 802.11 AĞLARININ ÖZELLİKLERİ

3.1. Modülasyon Yöntemleri

WLAN sistemleri lisans ve kullanım ücreti gerektirmeyen ISM (Industrial, Scientific, Medical) frekans bantlarında çalışmaktadır. Bu bantlar aynı zamanda telsiz servislerinin kullanımı için tahsisli olduğundan WLAN sistemleri enterferansa dayanıklı teknolojiler üzerine kurulmak zorundadır. Ayrıca, sınırlı frekans spektrumuna sahip bu bantların sistem ve kullanıcı ihtiyaçlarına cevap verebilecek şekilde verimli kullanılması gerekmektedir. Bu nedenlerle son yıllarda frekans spektrumunu verimli kullanan ve enterferanstan az etkilenen teknolojiler geliştirilmiştir. Aşağıda WLAN sistemlerinde kullanılan modülasyon teknolojileri açıklanmıştır [1].

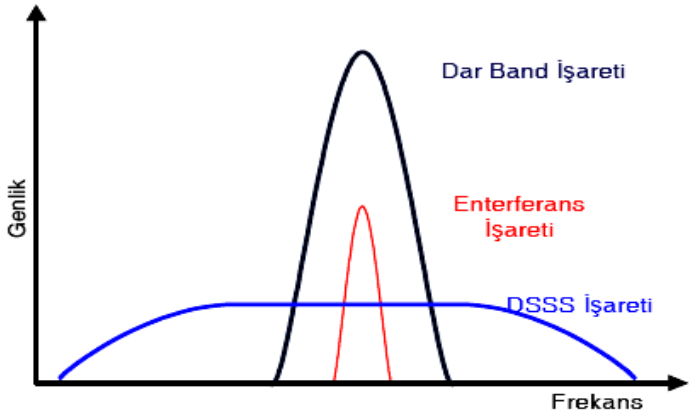
3.1.1. Darbant (narrowband) tekniği

Darbant tekniği, RF (Radio Frequency) sinyallerinin mümkün olan en dar frekans aralığında gönderilmesi ve alınması esasına dayanır. Bu yöntemde veri hızı düşük fakat iletişim mesafesi uzundur. Bu tür kullanımda her kullanıcının farklı frekans kanalı kullanması gerekir. Aksi durumda enterferans oluşur ve iletişimde bozulma veya kesilme meydana gelir. Özellikle yoğun kullanıcı bulunan bölgeler için uygun bir teknoloji değildir. Frekans talebinin ve kullanım yoğunluğunun az, iletişim mesafesinin uzak, veri hızının ise çok önemli olmadığı durumlarda ve kırsal alanlarda kullanılması mümkündür. Dar bant iletişim yöntemi WLAN sistemlerinde kullanılmamaktadır [1].

3.1.2. Geniş spektrum (spread spectrum) tekniği

Geniş spektrum (Spread Spectrum), kritik, güvenli ve gizli haberleşme sistemleri için geliştirilmiş bir kablosuz RF iletişim tekniğidir. Gönderilecek sinyal bir kod

kullanılarak belirli bir bandın tümüne yayılarak ya da önceden belirlenmiş bir düzende devamlı frekans atlatılarak gönderilir. Özel dizayn edilmiş alıcılar kaçak dinlemeyi engelleyen kodları temizleyerek istenilen iletişimi gerçekleştirirler. Bu yöntem gizlilik sağlamanın yanı sıra diğer telsiz sistemlerinden gelecek enterferansa karşı da sistemi dirençli kılmaktadır. Ancak, aynı teknolojiyi kullanan diğer sistemler tarafından verici kodlarında yanılgıya neden olarak kendisi kolayca etkilenebilir. İki çeşit geniş spektrum yöntemi vardır; FHSS ve DSSS [1,11].



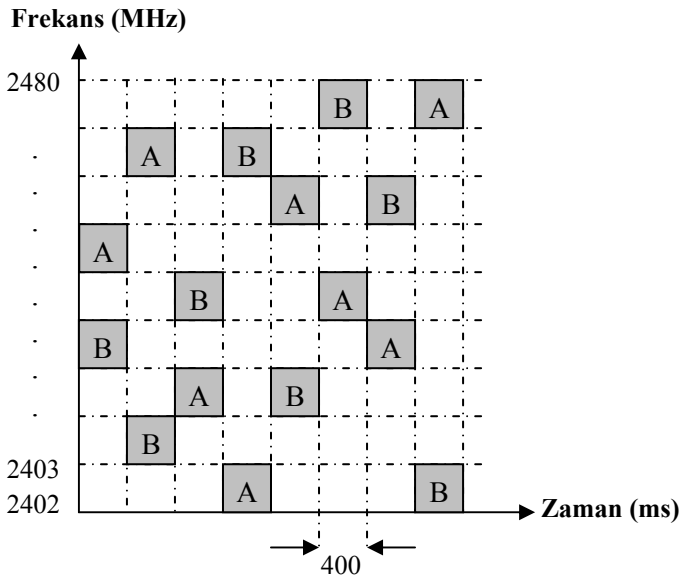
Şekil 3.1. Dar bant ve dağınık spektrum işaretleri [1]

3.1.2.1. Frekans atlamalı geniş spektrum (FHSS)

FHSS (Frenquency Hopping Spread Spectrum) tekniği, dar bant taşıyıcı sinyalinin rasgele ancak bilinen bir düzende bir frekanstan diğer frekansa atlayarak veri iletilmesi yöntemidir. Çalışma şekli şöyledir: verici bir atlama kodu seçerek sinyal gönderir. Atlama kodu frekansın değişimini belirleyen koddur. Bu sinyali alan alıcı da aynı atlama koduna ayarlanır. Böylece alıcı doğru zamanda doğru frekanstan gelecek sinyalleri almaya hazırdır.

FHSS tekniği için 2402-2480 MHz frekans aralığında 1 MHz aralıklarla 79 kanal bulunmaktadır. Bu sayı 75'ten az olmamak kaydıyla ülkeden ülkeye değişim göstermektedir. Bir atlama frekansındaki azami bekleme süresi 400 ms'dir. FHSS modülasyon tekniği IEEE 802.11 standardında kullanılmakta ve 2 Mbps'e kadar veri iletimi sağlamaktadır [1,7].

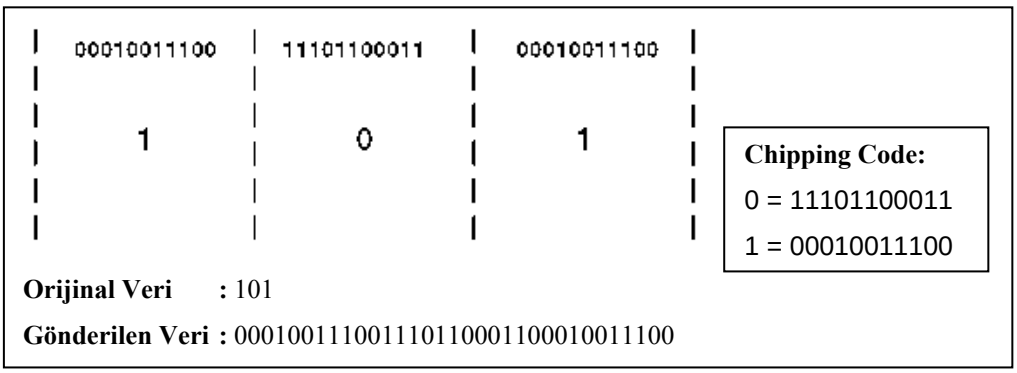
A ve B verilerinin FHSS tekniği kullanılarak iletilmesi Şekil 3.2'de gösterilmiştir.



Şekil 3.2. FHSS tekniği ile veri iletimi

3.1.2.2. Düz sıralı geniş spektrum (DSSS)

DSSS (Direct Sequence Spread Spectrum) tekniğinde, belirli bir frekans bandında sabit kalan bir taşıyıcı kullanılır. Veri, özel bir kodlama yöntemi kullanılarak çok daha geniş bir frekans bandında dağıtılır. Gönderilecek verinin her biti, çok daha fazla sayıda bit ile kodlanır. Çok sayıdaki bu bit dizisine "chip" ya da "chipping code" adı verilir. Verinin kodlanması Şekil 3.3'de gösterilmektedir.



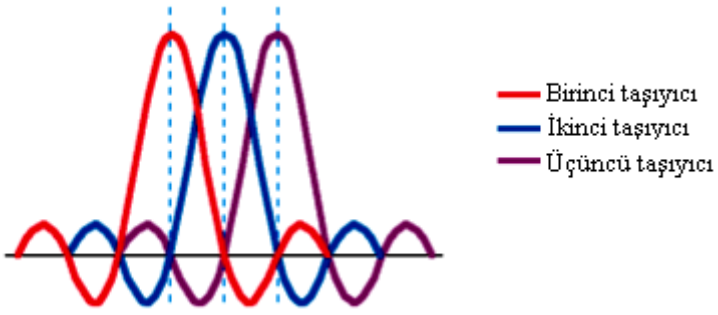
Şekil 3.3. DSSS tekniğinde verinin kodlanması

Kodlama sonucu elde edilen işaret, geniş bir frekans aralığında düşük güç seviyesinde iletilmektedir. Öyle ki; bu güç seviyesi gürültü seviyesinin altındadır. Bu, sistemin enterferansa karşı dayanıklı olmasını sağlamaktadır. Ayrıca, veri iletimi esnasında zarar gören veriler, istatistiksel yöntemler kullanılarak; orijinal veri, yeniden gönderilmeden (iletişim tekrarlanmadan) kurtarılabilmektedir [1,13].

FHSS ve DSSS teknikleri kıyaslanacak olunursa; DSSS, daha fazla bant genişliğine ve daha yüksek veri iletişim hızına sahiptir ve enterferanstan daha az etkilenmektedir. FHSS ise, daha güvenli bir veri iletişimine sahiptir ve aynı frekans bandında daha fazla erişim noktasının çalışmasına izin vermektedir [1].

3.1.3. Dikey frekans bölmeli çoklama (OFDM)

OFDM (Orthogonal Frequency Division Multiplexing), bir taşıyıcı yerine çok sayıda taşıyıcı kullanılan bir modülasyon tekniğidir. Bu teknikte RF sinyalleri daha küçük alt sinyallere bölünerek aynı anda farklı frekanslardan gönderilir. Şekil 3.4'de görüldüğü gibi OFDM alt sinyal taşıyıcıları birbirine dik açıyla üst üste binmekte ve böylelikle birbirine parazit yapmamaktadır. Ayrıca, bu teknikte sinyaller fiziksel engellerle karşılaştığında dağılmayıp, engelin çevresinden dolaşmaktadır.



Şekil 3.4. OFDM çalışma modeli [14]

OFDM modülasyonunun başlıca avantajları;

- Küçük bant genişliği kapladığından frekans spektrumunu verimli kullanır.
- Yüksek veri aktarım hızına sahiptir.
- İleri hata düzeltme algoritmaları ile iletilen verinin güvenliğini sağlar.

OFDM tekniği, bu avantajları ile birlikte WLAN sistemlerinde en çok kullanılan modülasyon yöntemidir [7,12,14].

3.1.4. Kızılötesi (infrared) teknolojisi

Kızılötesi teknolojisi gözle görülebilen ışığın altındaki frekansları veri iletiminde kullanan bir teknolojidir. Kızılötesi teknolojisini iki tür kullanmak mümkündür. Birincisi görüş hattı, ikincisi ise yansıma yöntemidir. Profesyonel olarak kızılötesi teknolojisi geçici ağ kurma ihtiyacı duyulan toplantılarda veya gezici satış elamanları tarafından kullanılmaktadır. Bu tür kullanımda yerel kablolu ağ ile bağlantı kurarak bilgi alış verişinde bulunmak ve sunucuya bağlı faks ve yazıcı gibi cihazlardan faydalanmak mümkündür.

Düşük güç tüketimi, RF sinyallerinden etkilenmemesi, kapalı ortamlarda yetkisiz dinlemeye ve bozucu etkilere karşı tam bir güvenlik sağlaması ve herhangi bir lisans gerektirmemesi kızılötesi teknolojinin avantajlarıdır. Dezavantajları ise; iletişim mesafesinin kısa olması (10-15 m), sinyallerin katı cisimleri geçememesi ve hava şartlarından etkilenmesidir [1].

3.2. Çoklu Erişim ve Çoğullama Yöntemleri

Radyo frekansı spektrumu sonlu bir kaynaktır. Bu yüzden aynı anda iletimde bulunacak uçbirimlerin kaçınılmaz bir şekilde belirli frekans aralıklarını paylaşmaları söz konusudur. Frekans spektrumun bölünmesi ve birçok kullanıcı arasında paylaştırmanın birkaç yolu bulunmaktadır. En basit ve açık yol Frekans Bölümlemeli Çoklu Erişim (Frequency Division Multiple Access, FDMA) yöntemidir. FDMA ile frekans spektrumu, frekans domeninde birbiri üzerine taşmayan bölmelere ayrılır. Bu bölmeler uçbirimlerin belirli bir çağrısı için elle veya otomatik olarak, uçbirimlere atanırlar. Örneğin 150 MHz'lik bir spektrum bloğu, 25 MHz bölmelere ayrılarak aynı anda altı uçbirimin eş zamanlı haberleşmesi sağlanabilir. Her bir çağrı için frekansı ayrı bir taşıyıcı işaret bulunacaktır. FDMA geleneksel olarak Analog sistemlerde yaygın bir şekilde kullanılmaktadır.

Zaman Bölümlemeli Çoklu Erişim (Time Division Multiple Access, TDMA) yönteminde ise, eldeki spektrum zaman domeninde bölmelere ayrılmaktadır. Yukarıdaki örnekteki 150 MHz'lik blok bu sefer altı zaman bölmeli ve tekrar eden çerçevelere ayrılacak, çerçevenin her bir altı gözünde altı farklı çağrıya ait bitler yer alacaktır. Başka bir deyişle uçbirimler eldeki spektrumun, birim zamanda kendilerine ait 1/6'lık bölümüne sıra ile erişebileceklerdir. Eğer çerçeveler yeterince hızlı tekrar edilirse uçbirimler haberleşme sırasında bir kesilme ve gecikmeyi hissetmeyeceklerdir.

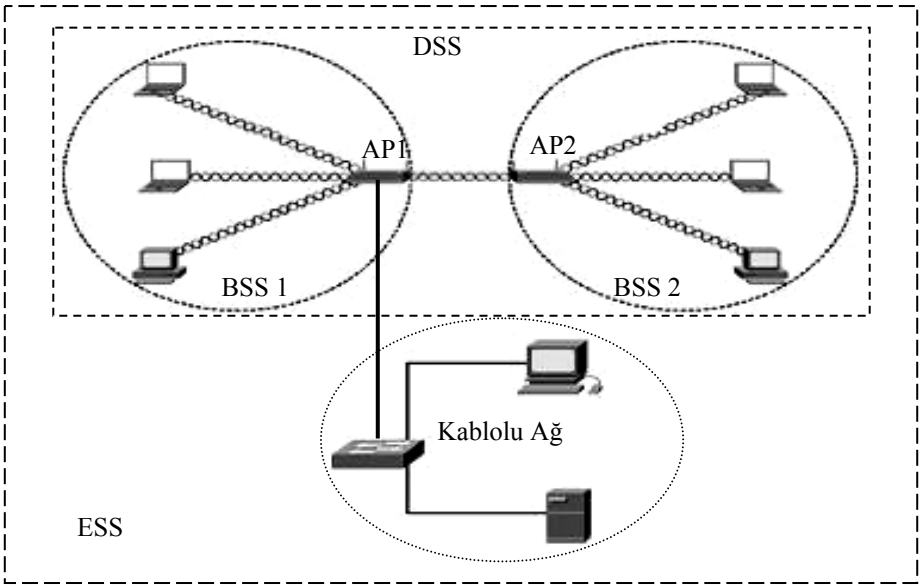
Üçüncü bir erişim yöntemi ise Kod Bölümlemeli Çoklu Erişim (Code Division Multiple Access,CDMA) olarak bilinir. Bu yöntem, dağılmış spektrum kavramına dayanan, hem bir modülasyon ve hem de bir erişim yöntemidir. Bir dağılmış spektrum sisteminde bilgi işaretinin taşınması için, bilgi işaretinin sahip olduğu bant genişliğinden çok daha geniş bir frekans aralığı kullanılır. CDMA sisteminde spektrum zaman veya frekans domeninde kanallanmaz. Bunun yerine çağrılar kodlama ile birbirlerinden ayrılırlar. Bu yaklaşımda iletimde bulunan her uç, her bir ayrı çağrı için benzersiz bir dağıtma kodunu, bilgi işaretini eldeki frekans aralığına yaymak için kullanır. Alıcı aynı benzersiz kodu kullanarak bilgi işaretini ayıklar; alıcı için diğer işaretler arka plan gürültüsü olarak algılanacaktır. Bu yolla aynı spektrum bloğunda aynı anda birden fazla çağrı gerçekleştirilebilir [13].

CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) birçok düğümden aynı andaki iletimden doğan çakışmaları en aza indirgeyen (fakat yok edemeyen) bir "konuşmadan önce dinle" ("listen before you talk") yöntemidir. CSMA/CA katılımcılarının sessizlik periyotlarında konuştuğu, eğer konuşma var ise sustuğu şeklinde geçen bir telekonferans gibidir. Bu, düğümlerin veri transfer etmek istediklerinde tüm bant genişliğini elde tutmaları anlamına gelir. Bununla birlikte ağa yeni düğümler eklendikçe kanalı elde etmek için çekişme artar, önemli bir süre olası çakışmaları çözmek için harcanır [7].

3.3. WLAN Topolojileri

Kablosuz ağlar, istasyonlar (STA – Stations) ve erişim noktaları (AP – Access Points) olmak üzere iki bileşenden oluşurlar. Kablosuz istasyonların diğer istasyonlarla iletişim şekline göre de iki farklı tipte kablosuz ağ çalışma modeli mevcuttur. Cihazdan cihaza (peer-to-peer ya da Ad-hoc) ve altyapı (infrastructure) çalışma modelleri.

Kablosuz ağları oluşturan en küçük yapı Temel Servis Kümesi (BSS – Basic Service Set)'dir. Bu temel yapıya "hücre" adı da verilmektedir. BSS'ler, diğer BSS'lerden ayrılmak için SSID (Service Set Identification) adı verilen özel bir kimlik numarası kullanırlar. BSS'lerin büyük ağlara (genellikle kablolu bir ağ) bağlanmasıyla oluşan yapıya Genişletilmiş Servis Kümesi (ESS – Extended Service Set), başka bir BSS'e bağlanmasıyla oluşan yapıya da Dağınık Servis Kümesi (DSS – Distribution Service Set) adı verilir [14,15,16].



Şekil 3.5 BSS, DSS ve ESS yapıları

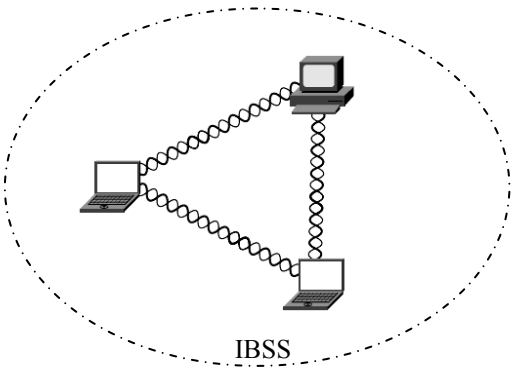
3.3.1. Cihazdan cihaza çalışma modeli (Ad-hoc)

Cihazdan cihaza çalışma modeli (Ad-hoc); iki ya da daha çok kablosuz iletişim özelliğine sahip bilgisayarın, bir sunucu (server) olmaksızın aralarında veri

iletişimine imkan veren ağ yapılarıdır. Bu modelde bilgisayarlar kendilerine ait dosya, yazıcı vb tüm kaynaklarını paylaşabilirler. Fakat bilgisayarlardan biri kablolu bir ağa bağlı olmadığı sürece, kablolu ağ veya internet kaynaklarını kullanamazlar.

Bu çalışma modelinde AP yoktur. Bilgisayarlar aralarında, kablosuz ağ kartları vasıtasıyla doğrudan haberleşirler. Bu yüzden hücreleri Bağımsız Temel Servis Kümesi (IBSS – Independent BSS) olarak adlandırılır. Bir başka deyişle IBSS, eşit düzeyde, istemci/sunucu ilişkisi olmayan bilgisayarlardan oluşur. İletişimi düzenleyen erişim noktasının olmaması dolayısıyla aynı anda birden çok haberleşme isteğinin çarpışmaya (collision) yol açması bu modelin dezavantajıdır.

Bu model çok yaygın kullanılmamakla birlikte geçici ve hızlı bir ağ ihtiyacı duyulan grup çalışmalarında ve toplantılarda kullanılmaktadır [1,14,15].



Şekil 3.6. Cihazdan cihaza (Ad-hoc) kablosuz ağı [15]

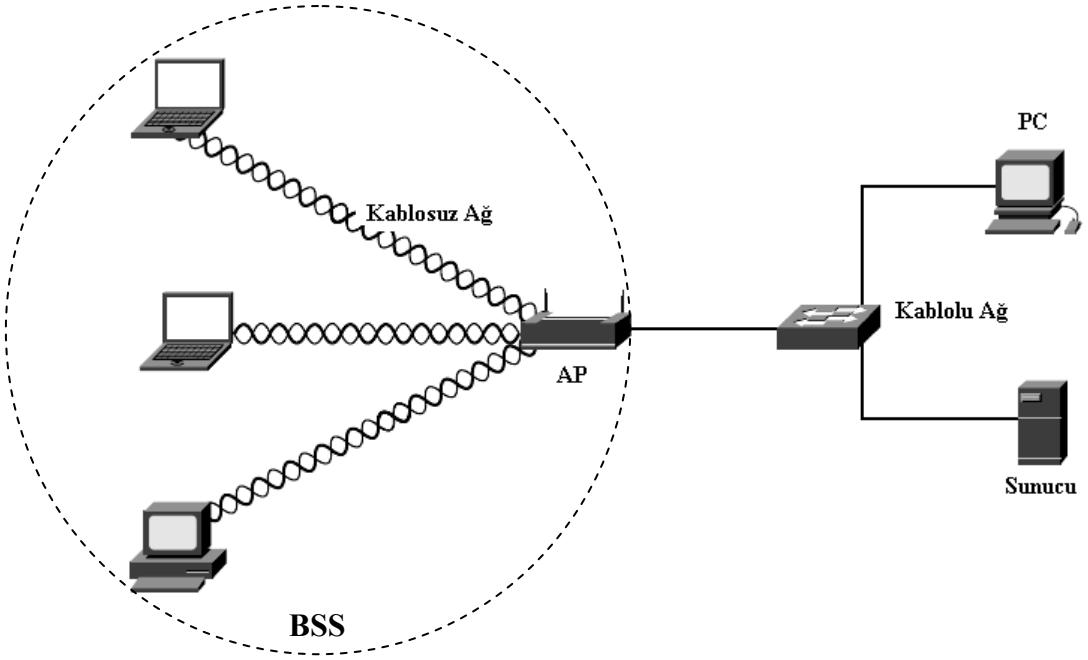
3.3.2. Altyapı (Infrastructure) çalışma modeli

WLAN sistemlerinin temel ve en yaygın kullanım şekli olan altyapı çalışma modeli; kablolu ağa bağlı bir AP ve istenilen sayıda kablosuz erişim özelliğine sahip cihazdan oluşur. AP, sadece kablosuz bilgisayarlar arasında değil; aynı zamanda kablolu bir ağa da bağlantı sağlar. Bir başka deyişle AP, kablolu ağlardaki anahtar ile aynı görevi yapar. Tipik bir AP radyo dalgaları ürüten bir cihaz, bir anten ve en az bir Ethernet portundan oluşur [15].

Bir AP, kullanıldığı teknolojiye ve konfigürasyonuna bağlı olarak 15-250 kullanıcıya 20-500 m mesafe aralığında hizmet sunar [7].

Diğer cihazların belirli bir erişim noktasına ulaşabilmeleri açısından doğal olarak söz konusu erişim noktasını diğer erişim noktalarından ayıran bir isme ihtiyaç duyulmaktadır. SSID adı verilen bu isim bir erişim noktasının kimliği durumundadır. Erişim noktası bu kimliği sürekli olarak yayınlayarak istemci cihazların kendisini tanımasını sağlar. SSID çevrede tüm cihazların görebileceği şekilde açık olarak yayınlanabileceği gibi gizli olarak da yayınlanabilir.

Bu çalışma modelinde paylaşılan bütün kaynaklar sunucuda yer alır ve işlemler sunucu aracılığıyla yürütülür. Sunucu işlemleri hızlı bir şekilde yaparak sonuçları istemciye yollar. Böylece işlem hızı ve kapasitesi artırılmış olur. Aksi durumda ise her bir bilgisayarın kendi programları ile verileri işlemesi gerekecektir. Bu durumda işlem hızı iş istasyonunun performansına bağlı olacaktır [14].



Şekil 3.7. Altyapı (infrastructure) kablosuz ağı [15]

3.4. WLAN Avantajları

3.4.1. Esneklik ve Genişletilebilirlik

Kablosuz teknoloji, ağların tasarımı, entegrasyonu ve konuşlandırılmasında çok büyük esneklikler sağlar. Kablolu bir ağın kurulu olmadığı yerlerde, alıcı-verici olarak çalışacak bir istasyon ve erişim noktası kurulumu ile kablosuz bir ağ uyarlamak çok basittir.

Kablolu ağlarda, kullanıcıların ağ kaynaklarına erişmesi için fiziksel bir yol gereklidir. Oluşturulan bu fiziksel yol sabittir; gerekli hallerde bilgisayarların yer değiştirmesi zordur ve genellikle yeniden bir kablolama gerektirir. Kuruluşlar, maliyet ve zaman kaybı dolayısıyla yeni bir kurulumu arzu etmezler.

Kablosuz ağ ile radyo dalgaları kullanılarak ihtiyaç duyulan bağlantı sağlanmaktadır. Radyo dalgaları duvarların, katların ve pencerelerin arasından geçtiği için fiziksel bir kablolama ihtiyacı yoktur ve bu, ağ mimarisinde çok büyük esneklik sağlar.

Kablosuz ağlarda; bilgisayarların montaj yerlerini tasarlamaya gerek yoktur. Sisteme yeni kullanıcıların katılması durumunda da ilave malzeme ve işçilik harcaması gerekmemektedir. Halbuki kablolu ağlarda ağa katılacak her yeni kullanıcı için yeni bir kablo çekilmesi gerekmektedir.

3.4.2. Dolaşım (Roaming)

Kablosuz bir ağın erişim bölgesi, onun kapsama alanıdır. Kablolu ağlarla karşılaştırıldığında, kablosuz ağ kullanıcılarının yerleşik olmasına gerek yoktur. Bir kullanıcı, Şekil 3.8'de görüldüğü gibi, AP'nin kapsama alanı içinde kablosuz ağa erişebilmektedir. Yine; Şekil 3.9'da gösterildiği gibi, kullanıcılar kablosuz ağa eklenen yeni bir AP'nin kapsama alanını da rahatlıkla kullanabilmektedir.

Bir ağa eklenen yeni AP'ler birbiri ile iletişim halindedir. Böylelikle eklenen her AP ağın kapsama alanını genişletmektedir. Kullanıcılar gerek fiziksel gerekse mantıksal

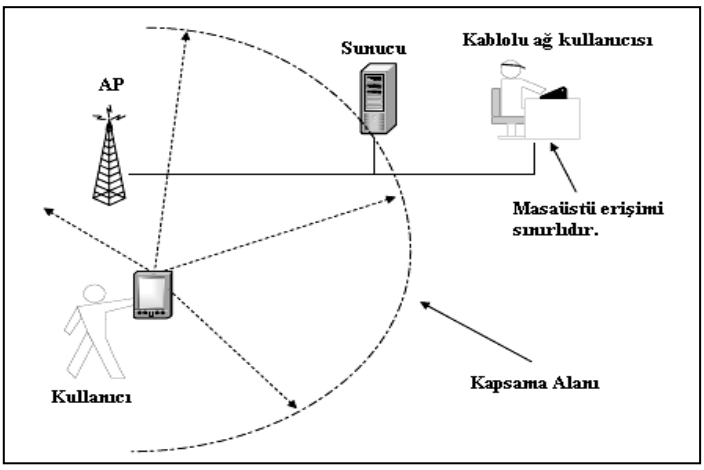
olarak ağ içinde bulunan herhangi bir AP'ye erişim sağlayabilirler. Her AP, ağda farklı görevler ve işlemler için özelleştirilebilir. Kullanıcıların bu farklı görev ve işlemlerden yararlanması için ilgili AP'nin kimlik doğrulama mekanizmasını geçmeleri yeterlidir.

Kullanıcıların bu hareket serbestliği içinde fiziksel ve mantıksal dolaşım ile ağ kaynaklarına ve verilere ulaşabilmesi kablosuz ağların en büyük yararlarından bir tanesidir. Şekil 3.10'da kullanıcının ağ içindeki dolaşım serbestisi gösterilmiştir.

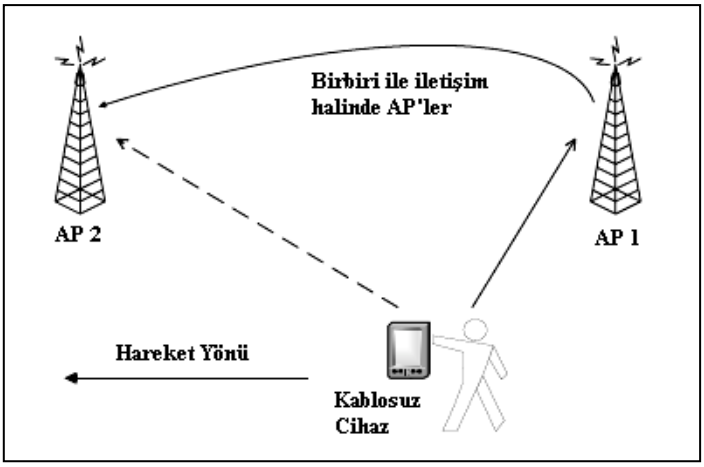
3.4.3. Taşınabilirlik

Taşınabilirliğin faydası, kuruluşların kablosuz ağ çözümlerine karar vermede tek başına büyük bir etkendir.

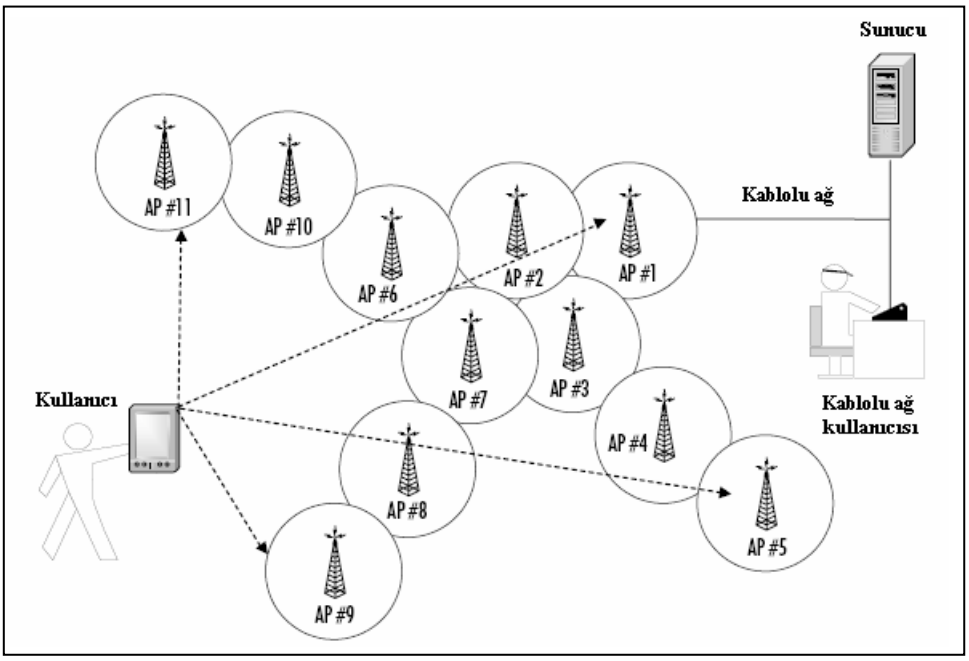
Kablolu ağlarda belirli bir yerde öncelikle bir kablo altyapısı oluşturulur. Çalışma alanının veya binaların değişmesi durumunda kullanıcıyla beraber bu yapının da taşınabilmesi çok kısıtlı olarak yapılabilir hatta bu çoğu durumda imkansızdır. Kablosuz ağlarda AP'ler elektriksel yollardan bağımsız olarak yeni bir mekana kolaylıkla taşınabilir ve aynı kablosuz ağ ekipmanları yeniden kullanılabilir. Örneğin; kablosuz bir ağ bir binadan başka birine farklı fonksiyonları gerçekleştirmek üzere taşınabilir. Bunu yaparken, ağ yöneticisi aynı ağ ekipmanlarını kullanarak daha modern bir ağ oluşturabilir.



Şekil 3.8. Kablosuz erişim [17]



Şekil 3.9. AP'ler arasında dolaşım [17]



Şekil 3.10. Bağlantılı erişim alanları [17]

3.4.4. Maliyet Kazancı

Kablosuz ağlar kurulacak sisteme göre değişmekle birlikte genellikle kablolu ağlara göre daha düşük maliyetlidir. Çünkü kablo maliyeti ve kablolama işçiliği ücreti yoktur. WLAN sistemlerinde kullanılan AP ve NIC kartlarının maliyeti ise her geçen gün biraz daha azalmaktadır. Genellikle spektrum kullanımı da ücretsizdir. Esnek ağ ihtiyacını karşılamada ve geçici ağ kurulumlarında WLAN sistemleri maliyet kazancı

sağlar. Kablo çekmenin zor olduğu doğal engellerin geçilmesi veya dağınık yapıya sahip kampüs uygulamalarında kurulum ve işletme maliyeti kablolu ağlara oranla düşüktür. Ayrıca kablo ve konektörlerin potansiyel arıza kaynağı olması dikkate alındığında WLAN sistemlerinde arıza oranı ve bakım gideri daha azdır. Özellikle fabrika ve depo gibi fiziksel şartların zor olduğu ortamlarda kablo arızası riski ortadan kaldırılmaktadır. Ağ idaresi açısından bakım maliyetlerinin düşüklüğü ve ağdaki bilgisayarların kolayca yer değiştirme imkanına sahip olması işletme ve bakım masraflarını en az düzeye indirmektedir.

3.4.5. Hız

Erişim hızı, hangi teknolojinin kullanılmasına karar verilirken göz önüne alınan önemli bir etkendir. Önceki kablosuz ağ standardı 3G; en fazla 2 Mbps erişim hızı sunmaktaydı. Bu hız, zengin çoklu ortam uygulamaları gibi yüksek hız gerektiren uygulamalarda yetersiz kalmaktaydı. Fakat yeni geliştirilen standartlar, bu hızı 54 Mbps mertebesine çıkarmıştır. Bu hız ise günümüz uygulamalarında yeterli bir hızdır. Ayrıca hızla gelişen kablosuz teknolojiler, kısa bir zaman zarfında daha yüksek hızlara ulaşılacağını vaat etmektedir.

Bu avantajlarının yanı sıra, ağ cihazları arasında kablolama olmaması, kablosuz ağlara estetik bir güzellik de katmaktadır [1,17].

3.5. WLAN Dezavantajları

Kablosuz ağ sistemlerinin pek çok avantajının yanı sıra bazı dezavantajları da bulunmaktadır.

Kötü niyetli saldırıları engellemek ve izinsiz kullanımları önlemek için bir güvenlik sistemine ihtiyaç duyulmaktadır. Çünkü havada serbestçe yayılan radyo dalgalarının doğası gereği dinlenmesini önlemek imkansızdır. Fakat son yıllarda geliştirilen güvenlik sistemleri, kablolu ağlardakine eşdeğer bir güvenlik vaat etmektedir. WLAN güvenlik sistemleri 4. bölümde geniş olarak incelenmiştir.

Diğer dezavantaj; kablosuz çalışan tüm sistemlerin enterferansa açık olmasıdır. Diğer kablosuz sistemlerin yanı sıra yakın noktalara yerleştirilecek AP'ler de kablosuz sistemde enterferansa neden olabilmektedir. Özellikle; kablosuz sistemlerin yoğun olarak kullanıldığı kamuya açık alanlarda bu sorun baş göstermektedir. Bu sorunun çözümü ise, ISM frekans bandı yerine özel tahsisli bantların kullanılması ile aşılabilir. Bu ise kablosuz ağ sistemine ekstra bir maliyet getirmektedir.

Diğer bir dezavantaj; kablosuz sistemlerin kapsama alanı ile ilgilidir. Kullanılan frekans bandı ve standartların müsaade ettiği kısıtlı çıkış gücü nedeniyle WLAN sistemlerinin mesafesi 100 m civarındadır. Bu mesafe açık alanlarda 300 m'ye kadar çıkabilmekle birlikte, duvar ve mobilya gibi fiziksel engellerin çok olması durumunda da 10 m'ye kadar düşebilmektedir. Bu sorunun çözümü için; AP'lerin kurulacağı noktalar çok iyi analiz edilerek kablosuz ağ oluşturulmalıdır. İyi bir planlama hem enterferansı en düşük seviyeye indirecek hem de kapsama alanındaki kopuklukları önleyecektir. Ayrıca kazançlı antenler kullanılarak kablosuz ağ kapsama alanı çok daha fazla artırılabilmektedir.

Bunların yanı sıra, taşınabilir bilgisayar sistemlerinin batarya kapasitelerinin birkaç saat ile sınırlı olması da kablosuz ağ sistemlerinin kullanımı açısından bir dezavantajdır. Batarya ömürlerinin artırılması bu sorunu ortadan kaldırmak için yeterli olacaktır. Ancak son yıllarda çok yaygın olarak kullanılan taşınabilir bilgisayarlar sadece kablosuz ağ sistemleri için değil diğer bütün sistem ve uygulamalar için bir batarya ömrü sorunu oluşturmaktadır [1].

3.6. WLAN Standartları

Bütün standartlarda olduğu gibi, WLAN standartları da geçen yıllar boyunca gelişim göstermiştir. Başlangıçta 900 MHz frekansında 1 Mbps veri iletişimine sahipken günümüzde 2.4 GHz ve 5 GHz frekanslarında 54 Mbps veri iletişimi hızına ulaşılmıştır [18].

WLAN standartları esas itibariyle ETSI (European Telecommunications Standards Institute), IEEE (Institute of Electrical and Electronics Engineers) ve MMAC

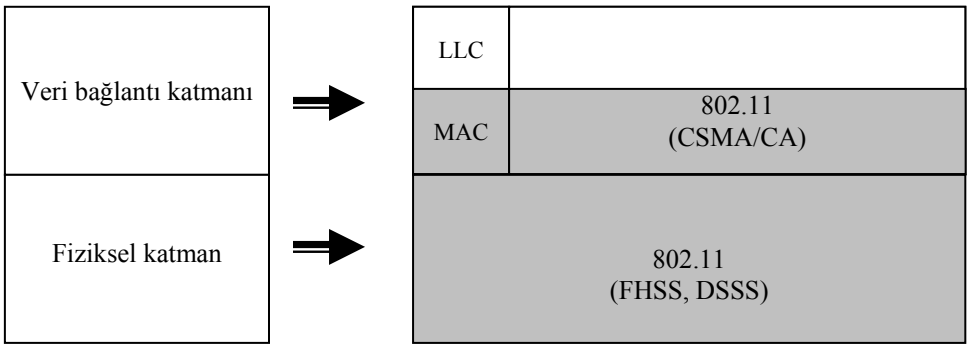
(Multimedia Mobile Access Communications Systems) olmak üzere üç kuruluş tarafından yürütülmektedir. ETSI Avrupa, IEEE Amerika ve MMAC ise Uzak Doğu'daki WLAN standartlarının oluşturulması konusunda çalışmaktadır. Bunların dışında değişik amaçlarla kurulmuş çok sayıda organizasyon bulunmaktadır. Bu organizasyonlar WLAN sistemlerinin tanıtımı, cihazların uyumluluk onayları, erişim alanları hakkında bilgi sağlanması ve benzeri konularda farklı hizmetler yürütmektedirler. Örneğin; eski adı WECA (Wireless Ethernet Compatibility Alliance) olan Wi-Fi Alliance (Wireless Fidelity Alliance), IEEE 802.11 standartlarında çalışan ürünlerin kullanımı ve benimsenmesini teşvik etmek ve sertifikalandırmak üzere kurulmuştur. Günümüzde en fazla, IEEE standartlarını esas alan kablosuz cihazlar ve teknolojiler kullanılmaktadır [1].

3.6.1. IEEE 802.11

IEEE, OSI referans modeline göre veri bağlantı katmanını MAC (Medium Access Control) ve LLC (Logical Link Control) olarak iki alt katmana ayırmıştır. Bunun nedeni üst katmanların, ağ donanım yapısına ve türüne bakmaksızın aynı arabirimle çalışabilmesini sağlamaktır [6].

802.11 standardı, IEEE tarafından 1997 yılında tanımlanmış temel WLAN standardıdır. Fiziksel katmanda ve MAC katmanında tanımlı olup 2.4 GHz ISM bandını kullanmaktadır. Bu standardın fiziksel katmanda, FHSS ve DSSS olmak üzere kullandığı iki farklı modülasyon yöntemi bulunmaktadır. Bu yöntem ile elverişli ortamlarda FHSS ile 2 Mbps, sinyal gürültüsü olan ortamlarda ise DSSS ile 1 Mbps veri iletim hızları sağlanmaktadır. Çok nadiren kullanılmakla birlikte kızılötesi teknolojisi de bu standart tarafından tanımlanmıştır. 802.11 standardı, MAC katmanında CSMA/CA erişim yöntemini kullanarak, sınırlı bant genişliğine sahip kablosuz iletim ortamını kullanıcılar arasında etkin bir şekilde paylaştırmayı hedefler [14,19].

IEEE, bu temel standardı daha yüksek veri iletim hızı, daha iyi servis kalitesi vb ihtiyaçları karşılamak üzere geliştirmeye devam etmiştir. Geliştirilen yeni standartlar, 802.11x adı ile tanımlanmış olup x bir harfi temsil etmektedir.

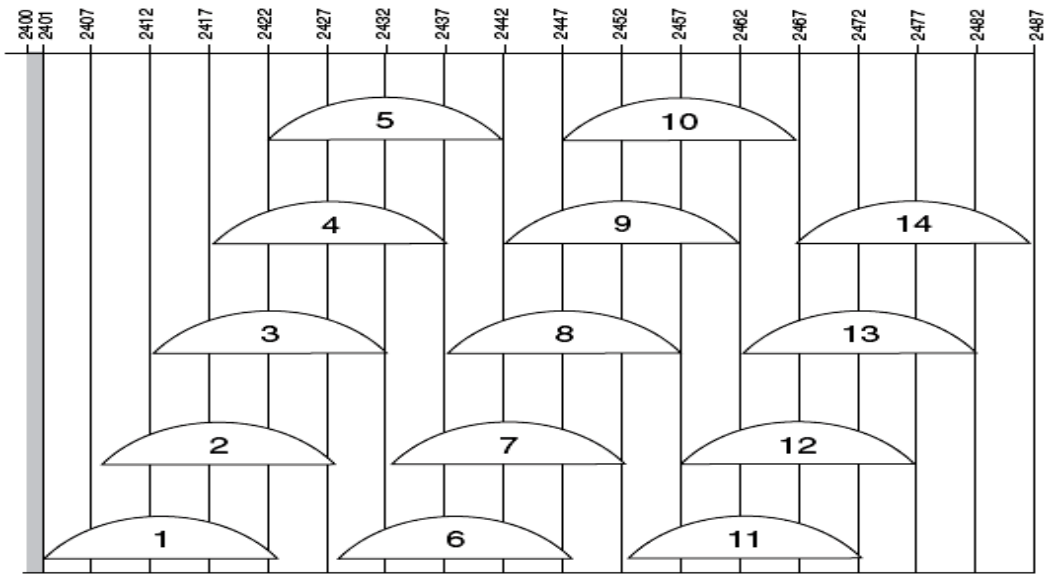


Şekil 3.11. OSI referans modeli ve 802.11 standardı

3.6.2. IEEE 802.11b

IEEE, temel 802.11 standardını geliştirerek 1999'da 802.11b standardı olarak yayınlamıştır. 802.11b standardı 2.4 GHz ISM bandında 1, 2, 5.5, 11 Mbps hızlarında çalışan ağ cihazlarını tanımlar.

802.11b, DSSS modülasyon tekniğini kullanır. 2.400'ten 2.487 GHz'e kadar 5 MHz aralıklarla 14 frekans kanalı mevcuttur. Kanal tahsisleri şeması Şekil 3.12'de gösterilmiştir. Şekilden de görüldüğü gibi birbiriyle çakışmayan 3 kanal vardır. 802.11b AP'ler farklı AP'ler ile birlikte aynı kapsama alanı içinde farklı kanallarda çalışabilirler. Böylelikle bant genişliği 3 katına çıkarılmış olur.



Şekil 3.12. 802.11b 2.4 GHz kanal tahsisleri [18]

802.11b standardı 1, 6 ve 11'nci kanallarda CSMA/CA erişim yöntemini kullanır.

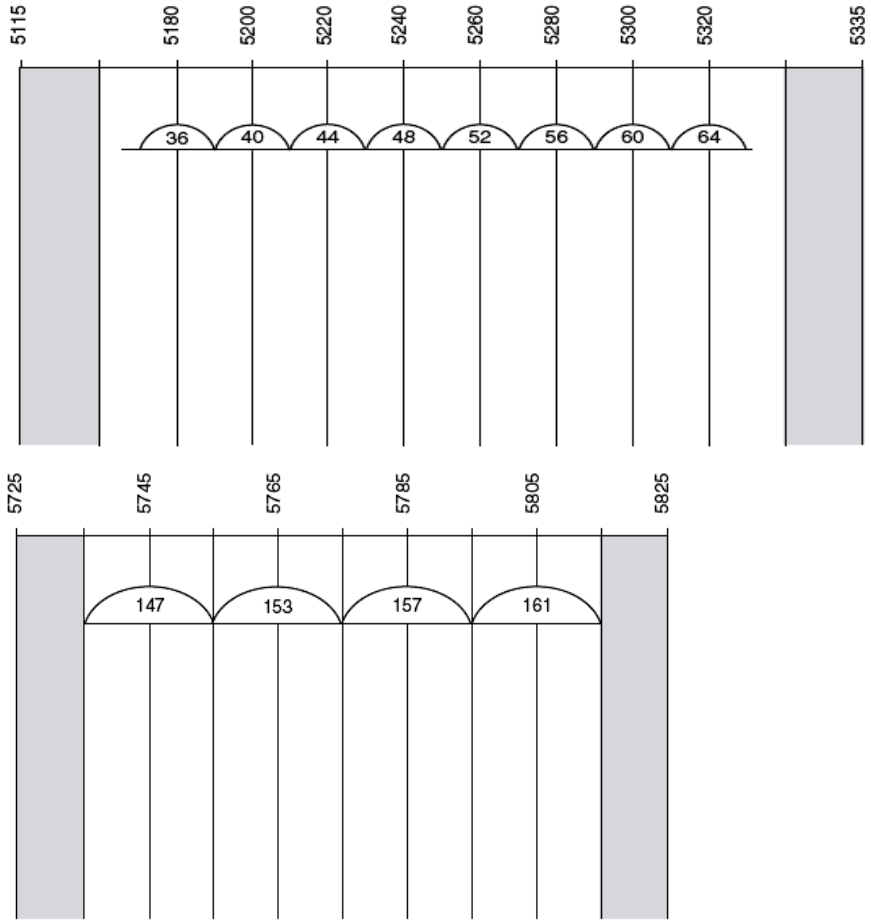
Gerek ağ erişim kartları (NIC) gerekse AP fiyatlarındaki düşüşler 802.11b standardını günümüzde en çok kullanılan standart haline getirmiştir. Bununla birlikte; aynı frekans bandı bluetooth, mikrodalga fırınlar, telsiz telefonlar ve amatör telsizler tarafından da kullanıldığı için 802.11b standardı enterferans sorununa çözüm bulmak zorundadır. Çünkü enterferans iletişim hızının düşmesine ya da kesilmesine neden olmaktadır [17,18,19].

3.6.3. IEEE 802.11a

IEEE, temel 802.11 standardında ikinci büyük düzenlemeyi 802.11a standardı olarak 1999'da duyurmuştur. 802.11a, 5 GHz frekansında 6, 9, 12, 18, 24, 36, 48, 54 Mbps iletim hızlarını destekler. Bu standartta veri aktarımında modülasyon tekniği olarak OFDM yöntemi kullanılmaktadır. OFDM modülasyon tekniği de benzer sistemlerden gelen enterferansa karşı duyarlıdır. Ancak 5 GHz frekans bandı diğer sistemler tarafından daha az kullanılmaktadır. Bu nedenle enterferans riski 2.4 GHz bandına oranla daha düşüktür. Ayrıca OFDM tekniğinin karakteristik özellikleri sayesinde, fiziksel engellerden dolayı oluşacak yansıma işaretleri kolaylıkla elimine edilebilmektedir. 802.11a standardında 20 MHz genişliğinde birbiriyle çakışmayan 12 kanal kullanılmaktadır. Bu da daha fazla bant genişliği anlamına gelmektedir. Kanal tahsis şeması Şekil 3.13'te gösterilmiştir.

5 GHz frekansının olumlu yanlarının yanında bazı olumsuz yanları da vardır. Yüksek frekanslı ağ ürünlerinin fiyatı daha yüksektir. Ayrıca yüksek frekanslarda kapsama alanı daha dardır ve yüksek frekanslı radyo dalgaları daha yüksek çıkış gücü gerektirirler. Bununla birlikte, 5 GHz frekansında çalışan bir AP, günümüzde daha sıklıkla kullanılan 2.4 GHz frekansında çalışan bir AP ile haberleşememektedir. Bu da, ağın farklı standartlardaki ürünlerle genişletilmek istenmesi durumunda ek bir AP kullanmayı gerektireceğinden maliyeti artırmaktadır.

Her şeye rağmen, yüksek hız gerektiren uygulamalar, 802.11a standardının önemini artırmaktadır [17,18,19].



Şekil 3.13. 802.11a 5 GHz kanal tahsisi [18]

3.6.4. IEEE 802.11g

IEEE 802.11g adını verdiği yeni bir kablosuz iletişim standardını 2003 yılında duyurmuştur. Bu standart 2.4 GHz standardını kullanması itibariyle 802.11b ile uyumlu olmakla birlikte veri transfer hızı itibariyle 54 Mbps veri aktarım hızına ulaşmaktadır. Bu standartta 802.11a standardında olduğu gibi modülasyon tekniği olarak OFDM kullanılmaktadır.

5 GHz frekans bandına göre daha düşük frekans bandı (2.4 GHz) kullanıldığı için cihaz üretimi daha kolay ve ucuz, RF sinyal zayıflaması ise daha azdır. 802.11g standardının en büyük dezavantajı ise 2.4 GHz bandının yoğun kullanılıyor olmasıdır. Bu yoğunluk kullanılabilecek boş kanal sayısının azalmasına, dolayısıyla iletişim kapasitesin düşmesine neden olmaktadır. 802.11g standardında da

802.11b'de olduğu gibi birbiriyle çakışmayan 3 kanal kullanılmaktadır. Ancak kanalların bant genişliği 22 MHz'dir [1,14,19].

3.6.5. IEEE 802.11h

Bu standart ile Avrupa'da geçerli 5 GHz WLAN düzenlemelerine uygunluk sağlamak için 802.11a standardına ek olarak MAC katmanına ilaveler yapılmıştır. Avrupa telsiz düzenlemelerine göre 5 GHz frekans bandında kullanılacak WLAN ürünlerinde TPC (Transmission Power Control) ve DFS (Dynamic Frequency Selection) özelliği bulunması zorunludur. 2002'de yayınlanan 802.11h standardının gelecekte 802.11a standardının yerini alması beklenmektedir [1,20].

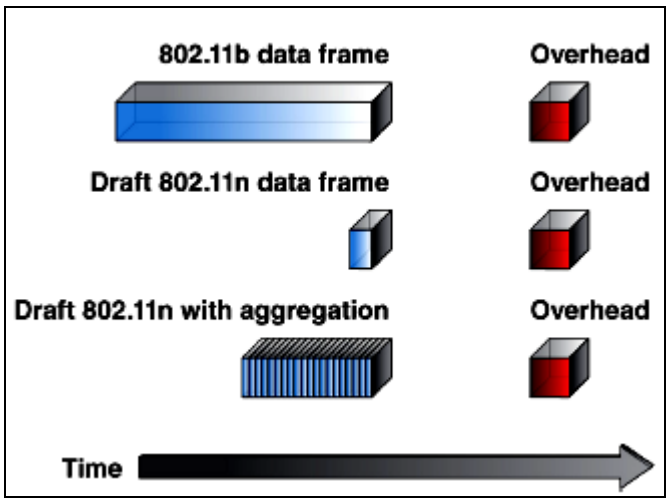
3.6.6. IEEE 802.11n

802.11n standardı Mayıs 2007 itibariyle halen tamamlanamamış ancak bu geliştirilme aşamasında taslak olarak duyurulmuştur. Günümüzde 802.11n taslağını destekleyen ürünler üretilmeye başlanmıştır.

Öncekilerden farklı olarak, bu yeni standardın hedefi IEEE 802.11 tarafından oluşturulmuş MAC katmanını geliştirmek ve PHY katmanında veri hızını artırmaktır. Bu standart ile en az 100 Mbps hız planlanmaktadır. Bu hedefe ulaşmak için 802.11n yeni bir MAC katmanı mekanizması tanımlar. IEEE bu amaçla üç büyük yenilik getirmektedir: Worldwide Spectrum Efficiency (WWise), Task Group N Synchronization (TGnSync) ve Mac and Mimo Technologies for More Throughput (MITMOT). Bütün bu yenilikler, veri hızını artırmak için MIMO (Multiple Input Multiple Output) ve yeni modülasyon-kodlama mekanizmaları kullanmaktadır.

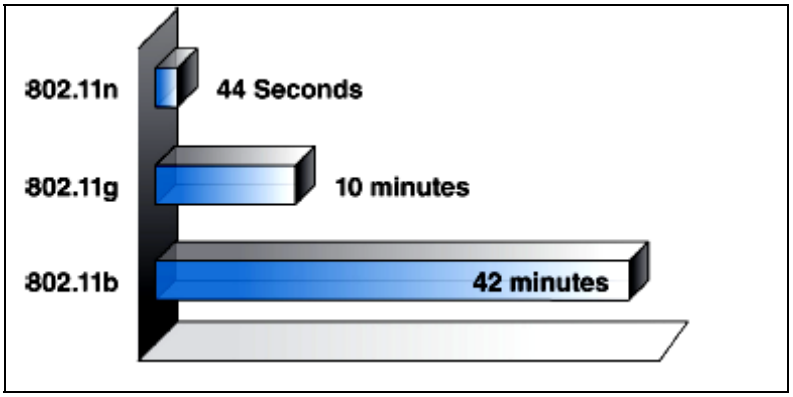
MIMO mekanizması iki alıcı ve iki gönderici (2X2) anten kullanılarak gerçekleştirilir. Bununla birlikte daha yüksek veri hızı ve daha kaliteli bir sinyal için (2X3) veya (2X4) şeklinde anten bağlantıları yapılabilir. 802.11n taslağına göre üretilen AP'ler hem 2.4 GHz hem de 5 GHz frekansında haberleşebilmektedir. Bu şekilde 802.11a, b, g standartları ile üretilmiş cihazlarla uyum içinde çalışabilecektir.

802.11n'deki yenilikler farklı modülasyon ve kodlama düzeneklerini beraberinde getirmektedir. WWise ve MITMOT 5/6 kodlama ile 64 durumlu QAM (Quadrature Amplitude Modulation) tekniğini getirirken TGnSync 7/8 kodlama ile 256 durumlu QAM tekniğini geliştirmektedir. Bu yenilik teklifleri, eski standartlarla uyumu sağlamak maksadıyla 20 MHz sabit bir bant genişliği kullanırlar. Bunun yanı sıra veri hızını artırmak için resmi olmayan yöntemlerle 40 Mhz bant genişliği de kullanılabilmektedir. (Örneğin Atheros Super-G).



Şekil 3.14. 802.11n ve 802.11b çerçevelerinin karşılaştırılması [9]

Kablosuz yerel alan ağlarında MAC katmanı verimliliğini artırmak için çeşitli mekanizmalar önerilmiştir. Taslağın son versiyonunda çerçeve bütünlüğü ve blok onayı prensiplerini getiren iki mekanizma geliştirilmektedir. Yürürlükteki IEEE 802.11 MAC katmanında, istasyon bir MAC çerçevesini gönderdikten sonra kısa bir süre bekler. Çerçeveler küçük ise bu bekleme zamanı ciddi bir boyuta ulaşmaktadır. Çerçeve bütünlüğü mekanizması, bu problemi en aza indirgemek amacıyla, küçük çerçeveleri daha büyük bir çerçeve içinde bir araya getirmesi için istasyonları yetkilendirir. Ayrıca bu yöntemin verimliliğini en üst dereceye çıkarmak için daha büyük çerçevelere izin veren maksimum çerçeve boyutu artırılmıştır. İkinci mekanizma olan blok onayı IEEE 802.11e servis kalitesi standardına uyum sağlamak amacıyla yine bu standarda benzer bir şekildedir [8,9,10].



Şekil 3.15. 30 dakikalık video görüntüsünün farklı standartlarda iletim zamanları [9]

3.6.7. IEEE 802.11c

Bu standardın görevi, AP'ler arasında köprüleme işlemlerini yapmaktır. Diğer 802.11 standartlarının MAC alt katmanında çalışır. Şirketler ve üniversiteler bu standardı, ağlarını genişletmek için sıklıkla kullanırlar [17,19].

3.6.8. IEEE 802.11d

802.11 standartları bazı ülkelerde yasal işletim haklarına sahip değildir. 802.11d'nin amacı kurallar koymak ve bu kurallar dahilinde WLAN uygulamalarını gerçekleştirmektir. Ağ cihazları üreticileri, ürünlerini bu standarda uyacak şekilde geliştirerek; ülkeden ülkeye farklılık gösteren kablosuz ağ uygulamaları için farklı özelliklerde cihaz üretmek zorunda kalmamaktadır [20].

3.6.9. IEEE 802.11e

802.11e standardı bütün 802.11 standartları için veri, ses ve görüntü iletişiminde servis kalitesini (QoS – Quality of Service) geliştirir ve artırır. MAC katmanında çalışan bir standart olmasına rağmen fiziksel katmanda çalışan standartlara destek verir [17].

3.6.10. IEEE 802.11f

Bu standardın ana görevi farklı üreticiler tarafından üretilen AP'ler arasındaki uyumluluğu sağlamaktır. Böylelikle kullanıcılar ağ içindeki farklı AP'leri kullanabilmektedir [20].

3.6.11. IEEE 802.11i

Bu standart, 802.11 standartları için güvenlik ve kimlik denetleme mekanizmaları geliştirir. MAC katmanında çalışır. Bir sonraki bölümde detaylı olarak anlatılacak olan bu standart, kablosuz ağlar için başlangıçta geliştirilen şifreleme standardını, algoritmasını vs tamamen değiştirmektedir.

3.6.12. ETSI HiperLAN

HiperLAN (High Performance Radio LAN), yüksek hıza sahip WLAN standardı olarak Avrupa ülkelerinde geliştirilmiştir. HiperLAN1 ve HiperLAN2 olmak üzere iki tipi vardır. Her iki tip de ETSI tarafından tanımlanmış olup, OFDM modülasyon yöntemi ile 5 GHz bandında çalışmaktadır. HiperLAN1 1996 yılının başlarında geliştirilmiş olup; 5 GHz frekans bandında 20 Mbps iletişim hızı sağlamaktadır. HiperLAN2 ise aynı frekans bandını kullanarak 54 Mbps hızına ulaşabilmektedir.

HiperLAN, 802.11 standartları ile benzer özellik ve kapasiteye sahiptir. Ancak 802.11 teknolojisi kadar yaygın değildir. HiperLAN2 ağlarında AP'lerden uç sistemlere bağlantıya yönelik bir yaklaşım vardır. Bu nedenle 802.11 standartlarından daha iyi servis kalitesine (QoS) sahiptir.

HiperLAN standardında TDMA erişim yöntemi kullanılmaktadır. Ayrıca kendine ait şifreleme ve kimlik denetleme mekanizmalarına da sahiptir [1,13].

Tablo 3.1. WLAN standartları ve genel özellikleri

Standart Adı	Modülasyon Türü	Erişim Yöntemi	Frekans Bandı	Veri Hızı (en fazla)	Kapsama Alanı
802.11	FHSS DSSS	CSMA/CA	2.4 GHz ISM	1-2 Mbps	30-150 m
802.11a	OFDM	CSMA/CA	5 GHz	54 Mbps	30-100 m
802.11b	DSSS	CSMA/CA	2.4 GHz ISM	11 Mbps	30-150 m
802.11g	OFDM	CSMA/CA	2.4 GHz ISM	54 Mbps	30-150 m
802.11h	OFDM	CSMA/CA	5 GHz	54 Mbps	30-100 m
HiperLAN1	OFDM	TDMA	5 GHz	20 Mbps	30-100 m
HiperLAN2	OFDM	TDMA	5 GHz	54 Mbps	30-100 m

BÖLÜM 4. 802.11 AĞLARINDA GÜVENLİK

4.1. Giriş

WLAN, kuruluşların içinde ve dışında esnek ve verimli bir yapı meydana getirmiştir. Envanter izleme, satış noktaları terminalleri, e-posta, internet erişimi gibi birçok uygulama kablosuz bağlantıdan yararlanmaktadır. Bununla birlikte, verimlilik artarken güvenlikle ilgili birçok tehdit de oluşmaktadır. Radyo dalgaları kuruluşların fiziksel sınırları dışına çıkmadıkça, kablosuz ağlar güvenlidir. Ancak bu fiziksel olarak mümkün değildir. Dışarıdan ağa sızabilecek yabancı bir kullanıcı veya kötü niyetli bir saldırgan da güvenli ağ bağlantısını tehdit etmektedir. Kablosuz ortam kendine has özelliklere sahip olsa da; kablosuz ağın güvenlik ölçütleri kablolu bir ağın güvenlik ölçütlerinden farklı değildir. Ağ yöneticileri, uygun güvenlik mekanizmalarını kullanarak kuruluşların gizliliğini temin edebilirler.

Ağ yöneticileri, WLAN ortamlarının güvenliği için uygun teknikleri bilseler de sürpriz bir tehditle karşı karşıya kalabilirler. Şirket yetkilendirilmiş bir WLAN'a sahip olsa bile kablolu ağ güvenliğini tehdit edebilecek kablosuz tehlikeler olabilir. Bu tehlikelerden en genel olanı yetkisiz bir AP'dir. Şirket çalışanlarından bazıları, tehlikelerden habersiz olarak hızlı kablosuz bağlantıdan yararlanmak maksadıyla kendi AP'lerini bilgisayarlarına bağlamaktadır. Bu tür AP'ler şirket güvenlik duvarının iç kısmında çalışırlar. Bu yüzden geleneksel yöntemlerle bu tür AP'leri tespit etmek çok zordur. Yetkisiz AP olarak adlandırılan bu AP'lerin kapsama alanındaki yetkisiz bir kullanıcı kolaylıkla şirket ağına girebilmektedir.

Diğer bir tehlike ise çalışanların işlerini yürütmek için ev, otel, hava alanı veya başka bir kablosuz erişim noktasından şirket ağlarına bağlanmasıdır. Bu durumda bu çalışanların bağlantısı, saldırgan için şirket ağına erişebileceği bir tünel vazifesi görebilir. Ayrıca kablosuz ağa üye bir kullanıcı yine aynı ağa üye diğer bir

kullanıcıya onun bilgisi dışında bağlantı kurabilir. Bu da güvenlik konusunda bir problem teşkil edebilir.

Şirketler, ağ güvenliklerini her türlü tehlikeye karşı sağlayabilmek için güvenlik stratejileri belirlemelidir. Kablolu ve kablosuz ağı korumak için, yetkilendirilmiş bir WLAN üzerinden gizli iletişim yapılmalıdır. Ağ üzerindeki her cihaz güvenli bir kablosuz bağlantı için yönetilebilir ve kontrol edilebilir olmalıdır. Şirketler ağlarını güvence altına almak için aşağıdaki ilkeleri uygulamalıdırlar:

1. Genel güvenlik ilkesini belirlemek
2. Güvenli bir WLAN kurmak
3. Ağı iç ve dış kaynaklı tehlikelerden korumak [21].

4.2. Genel Güvenlik İlkesi Belirlemek

İlk olarak kuruluşun bünyesine ne amaçla kablosuz bağlantıyı ekleyeceğini belirlemesi gereklidir. Daha sonra bu bağlantıya dışardan yapılabilecek sızmalara karşı ne gibi güvenlik önlemleri alınacağı kararlaştırılmalıdır. Ağa eklenebilecek her türlü yetkisiz cihaza karşı bir güvenlik politikası belirlenmelidir. Genel güvenlik ilkeleri aşağıdaki gibi sıralanabilir:

- Yetkilendirme ilkesi tanımlamak
- Sürekli destek veren uzman bir acil durum ekibinin olması
- Kablosuz ağı kullanacak kişilerin belirlenmesi (çalışanlar, misafirler vb.)
- Herhangi bir güvenlik ihlali durumunda raporlama ve önlem alma mekanizması geliştirmek
- Risk değerlendirmeleri yapmak ve tehlikelere karşı önlem almak
    - Verilerin ve ağ servislerinin güvence altına alınması
    - DoS (Denial of Service-servisin inkar edilmesi) saldırıları
    - Ağ cihazlarına zarar verilmesi veya onların çalınması
    - Yetkilendirilmemiş ağ erişimi
    - Şirketin gizli bilgilerinin çalınması
    - Çalışan bilgilerinin kayıtlı ve erişilebilir olması

  - Kötü niyetli verilerin araya girmesi
- Güvenlik için ayrılabilecek mali kaynağın belirlenmesi
- Dışarıdan yapılabilecek saldırılara karşı güvenlik ilkesi tanımlamak. Saldırı için kullanılan yöntemler:
    - Kablosuz ağ keşif mekanizmaları
    - Şifre yakalama ve kırma mekanizmaları
    - Ağ yönetim ve kontrol mekanizmaları
    - Kablosuz iletişim protokolü çözümleyicileri
    - Paylaşımdaki verilerin izinsiz kullanılması
    - İşletim sistemi port tarayıcıları
    - RF işaret bozma mekanizmaları
- Bağımsız güvenlik kuruluşlarının testlerine tabi olmak
- Güçlü bir şifreleme mekanizması kullanmak
- Sanal ağ oluşturmak [22].

4.3. Güvenli Bir WLAN Kurmak

Kablosuz ağlarda veriler radyo dalgalarıyla havadan iletilir. Kablolu ağlarda olduğu gibi fiziksel kablolamanın sağladığı özel kullanım durumu kablosuz ağlarda söz konusu değildir. İletişimin lisanssız frekans bantlarından yapılması, kablosuz ağların istenmeyen kişiler tarafından fark edilmesini sağlamaktadır. Mevcut teknolojiler kablosuz ağın yabancılar tarafından izlenmesine engel olamamaktadır. Ancak izlense dahi gerek veri içeriğine gerekse ağa erişimin engellenmesi izlenen güvenlik politikasıdır. Bu kapsamda, kablosuz ağlarda güvenliği sağlamak için aşağıdaki kriterlerin sağlanması gereklidir:

Asıllama (Authentication): Veri iletişimine başlamadan önce, kablosuz ağ düğümünün kimlik bilgilerinin geçerliliği denetlenmelidir. Böylelikle ağa sadece izin verilen kullanıcıların erişmesi sağlanır.

Şifreleme: Veri paketleri gönderilmeden önce, gizliliğin sağlanması için veriler şifrelenmelidir. Böylelikle istenmeyen kişiler tarafından verilerin deşifre edilmesi engellenir.

Veri bütünlüğü: Veri paketleri gönderilmeden önce, gerek alıcı gerek verici tarafında iletinin içeriğini kontrol eden ve sıralayan bir bilgi iletiye eklenmelidir. Böylelikle veri iletimi kontrollü bir şekilde yapılır ve saldırgan tarafından gönderilecek sahte veriler veri akışını bozamaz.

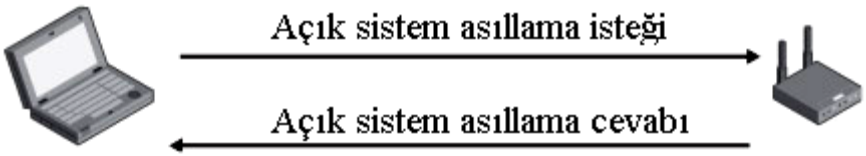
802.11 standardı kablosuz ağlar için asıllama, şifreleme ve veri bütünlüğü tekniklerini tanımlamıştır. Bu bölümde bu teknikler tarihsel gelişimine göre incelenecektir [23].

4.3.1. Asıllama (Authentication)

IEEE 802.11 iki tür asıllama tekniği tanımlamıştır.

- Açık sistem asıllama
- Ortak anahtarlı asıllama

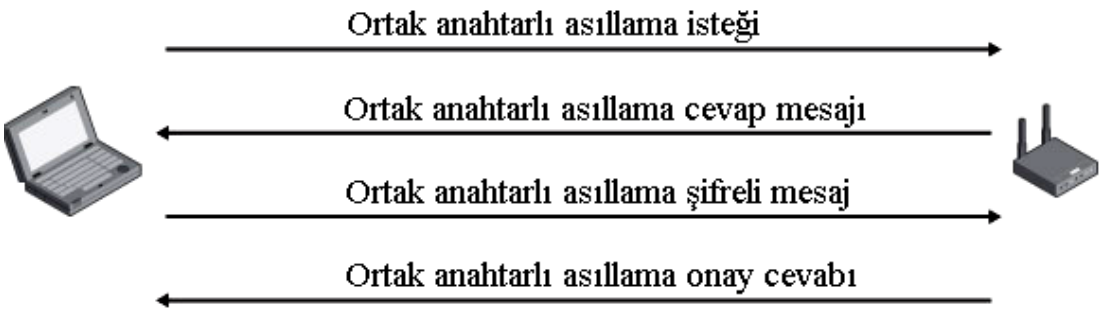
Açık sistem asıllamada kimlik denetimi yapılmaz. Kullanıcı erişim noktasından bağlantı isteminde bulunur, erişim noktası da isteği kabul eder. Bu yöntemde şifreleme kullanılmaz. Herhangi bir kısıtlamanın olmadığı ağlarda uygulanan bu yöntemin çalışma prensibi Şekil 4.1'de gösterilmiştir.



Şekil 4.1. Açık sistem asıllama

Ortak anahtar asıllama yönteminde, farklı olarak şifreleme kullanılır. İstemci AP'den istekte bulunur. AP rasgele bir mesajı istemciye gönderir. İstemci bu mesajı, kablosuz ağa kayıt olurken almış olduğu anahtar ile şifreler ve şifreli mesajı AP'ye

gönderir. AP almış olduğu bu mesajı kontrol ederek doğruluğunu denetler. Mesaj doğru ise bağlantıya izin verir [23].



Şekil 4.2. Ortak anahtarlı asıllama

Bu yöntemde hem istemci hem de AP tarafında önceden tanımlanmış statik bir anahtar kullanılır. Asıllama sırasında ve bağlantı sağlandıktan sonra bu statik anahtar kullanılarak iletişim sağlanır. Bu statik anahtarın bir saldırgan tarafından ele geçirilmesi halinde ağ, güvenliğini yitirecektir. Diğer bir sorun ise; yetkisiz bir AP'nin istemciden gelen isteğe cevap verebilmesidir. Diğer bir deyişle istemcinin bağlanmak istediği AP'nin kimliği hakkında hiçbir bilgisinin olmamasıdır. Ayrıca bu yöntemdeki asıllama, istemci ve AP cihazları arasındadır. Kullanıcı asıllaması yapılmamaktadır. Bu güvenlik açıklarını gidermek amacıyla 802.1x asıllama yöntemi geliştirilmiştir.

4.3.1.1. IEEE 802.1x asıllama

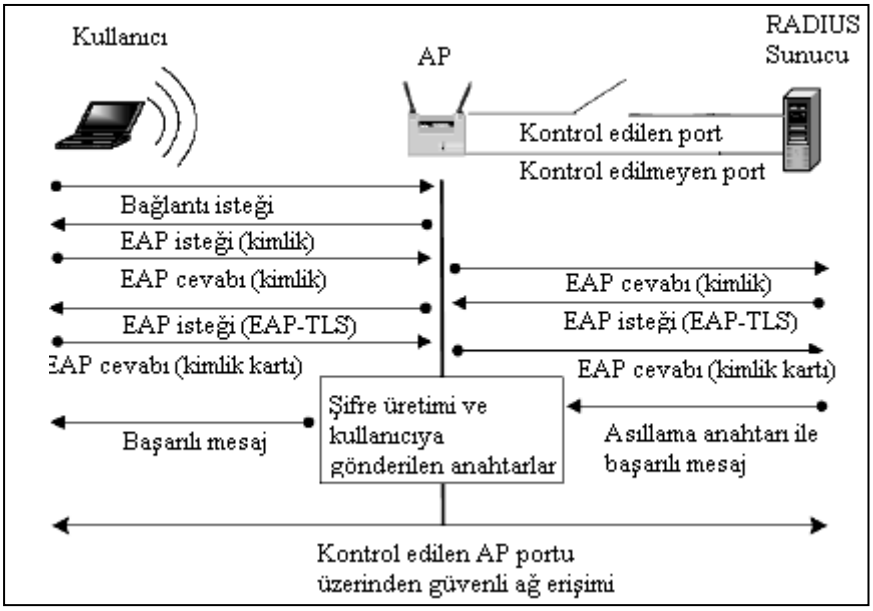
802.1x standardı IEEE tarafından geliştirilen port tabanlı güvenlik protokolüdür. Kablosuz ağda güvenliği temin etmek ve WEP'in (Wired Equivalent Privacy) zayıflıklarını gidermek için kablolu ağlarda kullanılan teknolojiden faydalanır. Bu standart ile ağ, kullanıcı, asıllayıcı ve asıllama sunucusu olmak üzere üçe ayrılır.

Ağ, anahtarlanmış LAN hub'larında olduğu gibi çok sayıda port içerebilir. İstemci ile port arasında birebir bir ilişki vardır ve her port bu ilişkiyi kontrol eden bir ilişkilendirilmiş asıllama mekanizmasına sahiptir. Portlar ile asıllama sunucusu arasında da bir ilişki vardır. Asıllama sunucusu her portun kendine has asıllama

kontrol mekanizmasından sorumludur. Asıllama sunucusu genellikle bir RADIUS (Remote Authentication and Dial-In User Service) sunucudur. Kimlik ve erişim bilgileri bu sunucuda saklanır.

802.1x asıllama işlemi şu şekilde gerçekleşir:

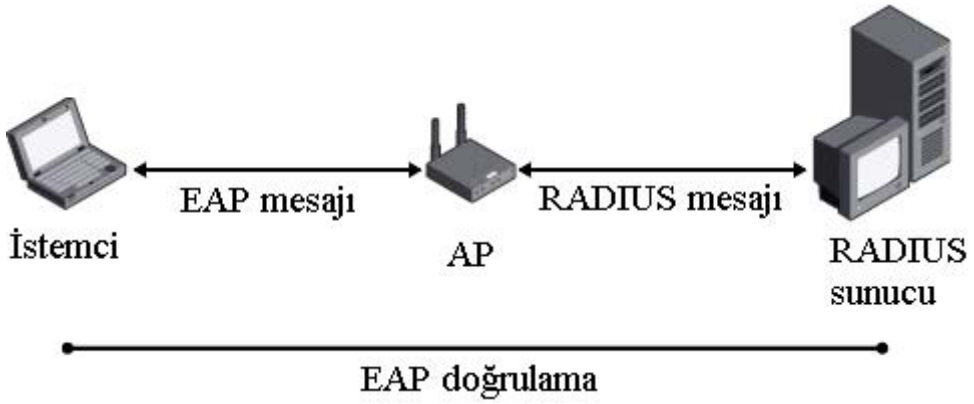
1. Kullanıcı kimlik bilgilerini göndererek AP'den erişim isteğinde bulunur.
2. AP, bu isteği kimlik kontrolü yapılmayan bir port üzerinden RADIUS sunucusuna iletir.
3. RADIUS sunucusu AP yolu ile kullanıcıdan talepte bulunur. Örneğin EAP-TLS mekanizmasını kullanarak,
4. Kullanıcı, AP yoluyla RADIUS sunucusuna kimlik bilgilerini cevap olarak iletir.
5. Kimlik bilgileri doğru ise, RADIUS sunucusu AP'ye şifrelenmiş bir asıllama anahtarı gönderir.
6. AP, sadece o oturumda kullanılabilecek şifrelenmiş bir asıllama anahtarını kullanıcıya gönderir.



Şekil 4.3. 802.1x asıllama işlem adımları [24]

Kullanıcı AP'ye üye olsa bile kimlik doğrulaması işlemini geçmeden ağa bağlanamaz. Bu yöntemde istemci AP'nin AP de istemcinin güvenilirliğini kontrol etmektedir. Dolayısıyla karşılıklı (çift yönlü) bir asıllama söz konusudur. Aynı zamanda sunucunun raporlama özellikleri merkezi bir yönetim sağlamaktadır. 802.1x standardında bunlara ek olarak dinamik şifreleme mekanizması kullanılmaktadır [24,25].

İstemci-AP-RADIUS arasındaki iletişimi tanımlayan 802.1x standardı mevcut diğer standartları da kullanmaktadır. Şekil 4.4'te gösterildiği gibi EAP (The Extensible Authentication Protocol) ve RADIUS iletişim standartları güvenliğin sağlanmasında büyük rol oynamaktadır.

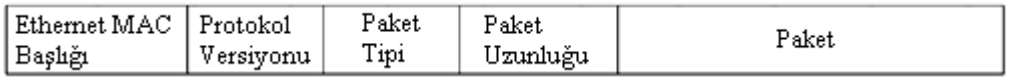


Şekil 4.4. 802.1x asıllama

4.3.1.2. EAP

EAP, RADIUS sunucu ve kullanıcı arasında AP yolu üzerinden, talep ettikleri asıllama işlemini gerçekleştirmek için kullanılır. MAC alt katmanında çalışır ve standart asıllama mekanizmasına PPP (Point-to Point Protocol) tarafından sağlanan farklı bir asıllama yöntemi ekler. PPP asıllama protokolü CHAP (Challenge Handshake Authentication Protocol) gibi özel asıllama mekanizmalarının kullanılmasını sağlar. EAP kullanımında PPP ile güçlü bir asıllama gerçekleştirilebilir. Asıllama esnasında sabit mesaj serileri kullanıcı ve sunucu arasında özel bir düzende gönderilir.

EAP esasen modem yolu ile dial-up asıllama için tasarlanmıştır. EAP mesajlarının WLAN'lara uyarlama işlemini 802.1x standardı EAP over LAN (EAPOL) ile tanımlamıştır. EAPOL çerçeveleri EAP mesajlarını sunucu ve kullanıcı arasında taşır. EAPOL mesajlarının yapısı Şekil 4.5'te gösterilmiştir.



Şekil 4.5. EAPOL çerçeve yapısı

Farklı EAP kimlik doğrulama protokolleri vardır. 802.1x destekli bu protokollerin yanı sıra üretici firmaların geliştirdiği farklı yöntemler de bulunmaktadır. Bu protokollerden bazıları şunlardır:

EAP-TLS (EAP-Transport Layer Security): EAP-TLS Internet Engineering Task Force (IETF) standardıdır. Asıllama için hem kullanıcı hem de sunucu tarafında X.509 dijital sertifika kullanır. Dijital sertifikalar bir kayıt defterinde veya akıllı kart gibi bir cihazda saklanır. EAP-TLS karşılıklı asıllama işlemi şu şekilde yapılır:

1. Kullanıcı AP'ye üye olur.
2. Tüm erişim istekleri asıllama yapılana kadar bloklanır.
3. Kullanıcı, dijital sertifika ile sunucuyu asıllar.
4. Sunucu, dijital sertifika ile kullanıcıyı asıllar.
5. Sunucuda ve kullanıcı kartında dinamik bir WEP anahtarı oluşturulur.
6. Sunucu bu anahtarı güvenilir kablolu ağ üzerinden AP'ye gönderir.
7. AP ve kullanıcı tek kullanımlık bu anahtarı aktif hale getirirler ve iletişim esnasında kullanırlar.

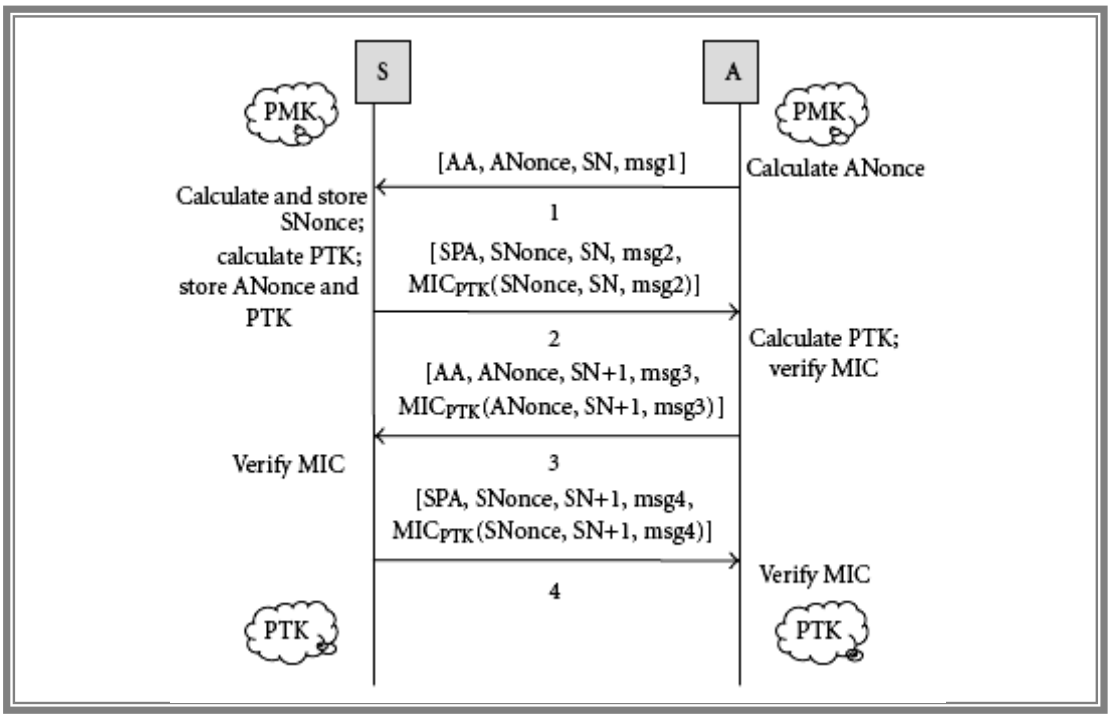
PEAP (Protected EAP): IETF tarafından oluşturulan taslak temel alınarak Cisco Systems, Microsotf ve RSA Security tarafından geliştirilmiş bir protokoldür. EAP-TLS protokolüne benzer. Farklı olarak sunucu, kullanıcıyı dijital bir sertifika ile asıllamaz. Bunun yerine tek kullanımlık şifre vs değişik yöntemler kullanılır.

LEAP (EAP-Cisco): Cisco tarafından geliştirilmiştir. Asıllama esnasında dijital sertifika kullanılmaz. Bunun yerine; kullanıcı, "kullanıcı adı" ve "şifre" bilgilerini girer. Sunucu da kullanıcıyı asıllar. Tek kullanımlık şifre desteği yoktur [15,23,24,25].

4.3.1.3. Oturum anahtarı üretimi

802.1X/EAP asıllama mekanizması, dinamik bir oturum anahtarı üreterek kullanıcı ile AP arasındaki haberleşmenin güvenliğini sağlamaya çalışır. Bu amaçla, kullanıcı, erişim noktası ve sunucu tarafından başlangıçta bilinen bir ana anahtardan (PMK – Pairwise Master Key) yararlanılır. PMK anahtarı 256 bit uzunluğundadır. Bu anahtar, kullanıcı ile asıllayıcının asıllama işlemi esnasında, veri iletişiminde kullanacakları geçici oturum anahtarını üretmelerinde kullanılır. Ancak, kablosuz ağda bir sunucu bulunmaması durumunda PMK yerine WEP'te olduğu gibi statik bir anahtar (PSK – Preshared Key) kullanılmaktadır. Geçici oturum anahtarı PTK (Pairwise Transient Key) olarak adlandırılır ve 512 bit uzunluğundadır.

PTK anahtarının üretilmesi çok önemlidir. Çünkü bu işlem aynı zamanda asıllama işleminin tamamlanmasında da etkilidir. PTK anahtarının üretilmesi dörtlü anlaşma (handshake) adı verilen bir protokol ile gerçekleştirilir. Şekil 4.6 PTK anahtarının dörtlü anlaşma protokolü ile üretilmesini göstermektedir.



Şekil 4.6. Dörtlü anlaşma protokolü [31]

Dörtlü anlaşmada, sadece 4 tür mesaj tanımlanmıştır. Bu mesajlar:

Msg1 : [AA, ANonce, SN, Msg1]
Msg2 : [SPA, SNonce, SN, Msg2, MIC(SNonce, SN, Msg2)]
Msg3 : [AA, ANonce, SN + 1, Msg3, MIC(ANonce, SN + 1, Msg3)]
Msg4 : [SPA, SNonce, SN + 1, Msg4, MIC(SNonce, SN + 1, Msg4)]

S : Kullanıcı,
A : Asıllayıcı,
MIC : Mesaj bütünlük kodu,
AA : Asıllayıcının MAC adresi,
SPA : Kullanıcının MAC adresi,
ANonce : Asıllayıcı (AP) tarafından üretilen rastgele bir değer,
SNonce : Kullanıcı tarafından üretilen rastgele bir değer,
SN : Mesajın sıra numarası,
MsgX : Mesaj X'in tipini tanımlar.

Dörtlü anlaşma protokolü “Nonce” değerlerinin üretilmesiyle başlar. Bu değerler sadece bir kez üretilir. Asıllayıcı (A) ANonce değerini Msg1 içine koyarak kullanıcıya (S) iletir. Kullanıcı Msg1 mesajını aldıktan sonra, AA, SN ve ANonce değerlerini bilecektir. Bu aşamada, kullanıcı SNonce adında yeni bir rastgele değer üretir; ANonce, SNonce, AA, SPA, PMK veya PSK değerleri PRNG (pseudorandom) fonksiyonu ile şifrelenerek PTK değeri hesaplanır. Bu PTK değerinden de Msg2 mesajı ile birlikte gönderilecek MIC değeri hesaplanır.

PTK ve MIC değerleri hesaplandıktan sonra kullanıcı, ANonce, SNonce ve PTK değerlerini saklar ve Msg2 mesajını asıllayıcıya gönderir. Asıllayıcı Msg2 mesajını aldıktan sonra, SNonce değerini bileceği için, kullanıcı ile aynı prosedürü kullanarak PTK değerini hesaplayabilir. Asıllayıcı, hesapladığı bu PTK değerini kullanarak MIC değerini hesaplar ve bu değeri Msg2 mesajı içinde aldığı MIC değeri ile karşılaştırır. Her iki MIC değeri eşitse kullanıcı onaylanır ve asıllayıcı Msg3 mesajını kullanıcıya gönderir. Kullanıcı da aynı şekilde MIC değerini onayladıktan sonra Msg4 mesajını asıllayıcıya gönderir ve dörtlü anlaşma tamamlanır.
Dörtlü anlaşma protokolü bunların dışında, aşağıda sıralanmış güvenlik önlemlerini de içermektedir:

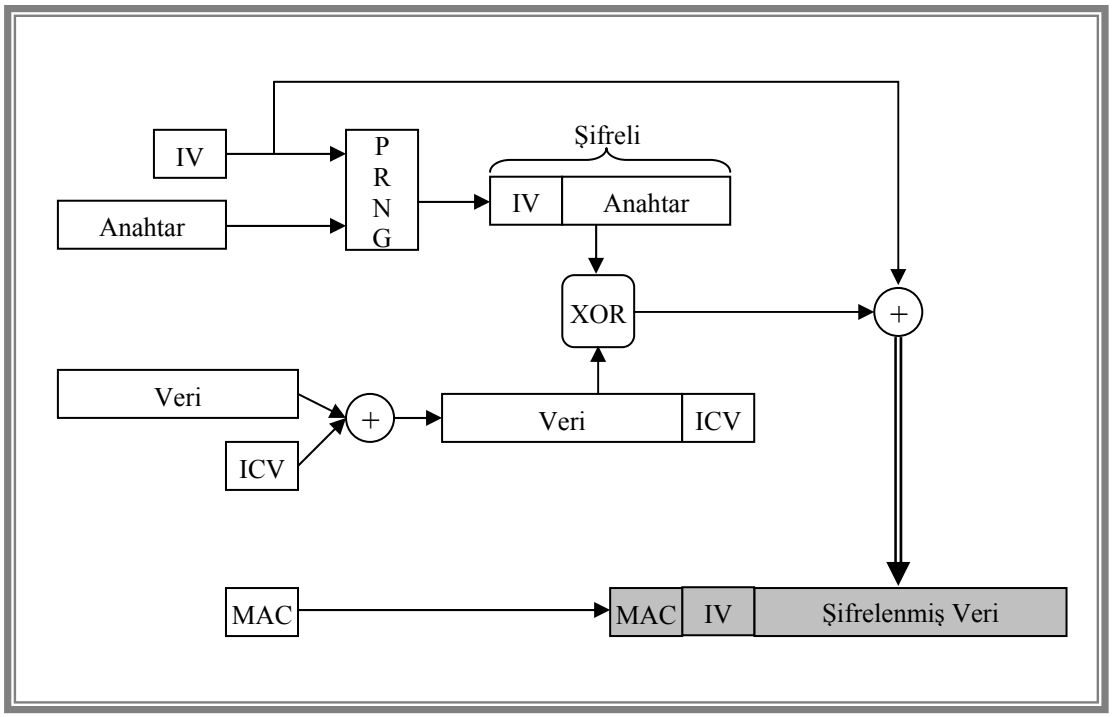
1. Kullanıcı ve asıllayıcı geçerli olmayan bir SN veya MIC değeri içeren mesaj alırlarsa, bu mesajı dikkate almayacaklardır. Bu yaklaşımla Man In The Middle (Ortadaki Adam) saldırılarından korunmak amaçlanmaktadır.
2. Kullanıcı, Msg1 mesajını bir zaman damgası ile birlikte almazsa, bu mesajı dikkate almayacak, asıllama yapmayacak ve asıllama prosedürü yeniden başlayacaktır.
3. Asıllayıcı, Msg2 veya Msg4 mesajını bir zaman damgası ile birlikte almazsa, Msg1 veya Msg3 mesajını tekrar göndermeyi deneyecektir ve belli bir deneme sonunda kullanıcı ile bağlantısını kesecektir [31,32].

4.3.2. Şifreleme ve veri bütünlüğü

4.3.2.1. WEP

Wired Equivalent Privacy (WEP), 802.11 standardıyla beraber geliştirilmiş olan temel güvenlik birimidir. Kablosuz düğümler arasındaki iletimde şifreleme ve veri bütünlüğünü sağlama işlemlerini gerçekleştirmeye çalışır. RC4 şifreleme algoritmasını kullanır. WEP şifreleme için kullanıcı ve erişim sağlayıcı tarafında 40 bitlik statik bir anahtar tanımlanır. Ayrıca WEP, akış şifresini elde etmek için 24 bitlik bir ilklendirme vektörü (Initialization Vector – IV) kullanılır. WEP'in çalışması şu şekildedir:

1. Veri bütünlüğünü sağlamak amacıyla, veri bir doğrulama algoritmasına (integrity check) tabi tutularak, doğrulama bitleri (ICV – Integrity Check Value) elde edilir.
2. Bu doğrulama bitleri verinin sonuna eklenir.
3. 24 bitlik IV statik anahtarın başına eklenir; 64 bitlik paket oluşturulur.
4. 64 bitlik bu paket RC4 (rastgele sayı üretici – PseudoRandom Number Generator-PRNG)) algoritması ile şifrelenir.
5. 2. adımda elde edilen veri ile 4. adımda elde edilen veri bir XOR işleminden geçer.
6. Elde edilen bu verinin başına tekrar IV eklenir ve iletilecek şifreli veri elde edilir. Şifreli verinin elde edilmesi Şekil 4.7'de gösterilmiştir. Elde edilen bu verinin başına, alıcı ve vericinin MAC adresi eklenerek kablosuz ortama gönderilir.
7. Şifreli veri, karşı tarafta aynı işlemler tersi yönde uygulanarak açılır.



Şekil 4.7. WEP şifreleme akış diyagramı

WEP şifreleme tekniği birçok güvenlik açığı barındırmaktadır. Saldırganlar, günümüzde WEP ile şifrelenmiş verileri kolaylıkla deşifre edebilmektedir.

WEP'in zayıflıkları:

WEP'te kullanılan ortak anahtar, herhangi bir şekilde istenmeyen bir kişi tarafından elde edilebilir. Ortak anahtara sahip bir kullanıcı ağı istediği gibi kullanabilmektedir.

WEP, RC4 algoritmasına parametre olarak ortak anahtar ile beraber IV'ü geçirmektedir. IV değeri her paket için değişmektedir. Başlangıçta sıfır değerindedir ve her işleme girdiğinde değeri bir artar. 24 bit uzunluktaki IV, 2^{24} farklı değer alır. Böylece RC4 algoritmasından 2^{24} tane farklı akış şifresi elde edilmiş olunur. Dolayısıyla 2^{24} paket sonra aynı IV değerleri tekrar kullanılacaktır. Ağı dinleyen bir saldırgan, tekrar eden bu verileri alarak istatistiksel yöntemlerle veriyi deşifre eder.

Diğer bir zayıflık, PRNG algoritması ile oluşturulan akış şifrelerinin doğrusal bir yöntemle oluşturulması ve dolayısıyla bu şifrelerin çözülmesinin kolay olmasıdır.

İletilen verinin baş kısmındaki MAC adres bilgileri şifrelenmez. Saldırgan bu adresleri istediği şekilde değiştirerek verileri farklı bir adrese yönlendirebilir.

WEP'te tekrar saldırılarına karşı alınan herhangi bir önlem de yoktur. Araya giren bir saldırgan asıllama işleminde gönderilen veriyi, daha sonra AP'ye göndererek kendini sisteme kayıt ettirebilir.

WEP'teki bu zayıflıkları gidermek için IV 128 bite, ortak anahtar 104 bite çıkarılmıştır. Ancak bunlar da WEP'in kırılmasını engelleyememiştir [16,17,25,26].

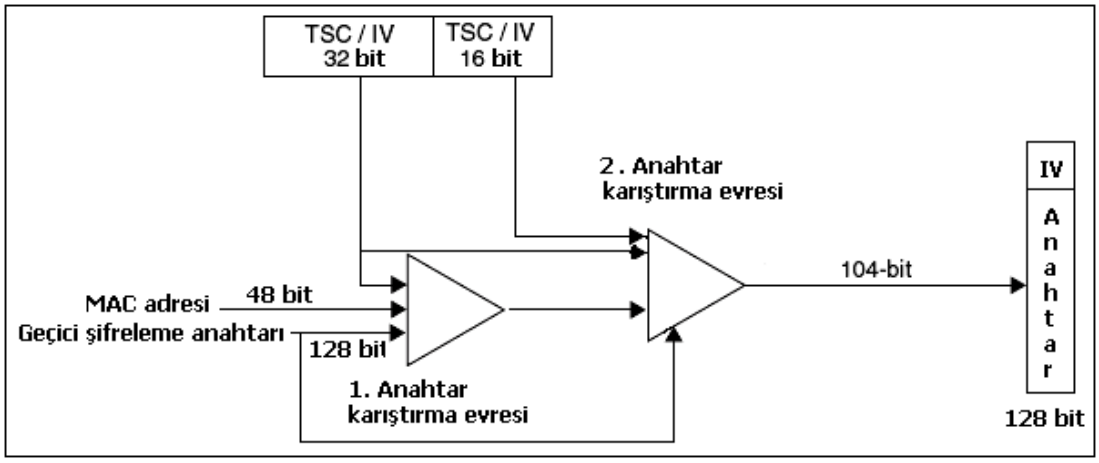
4.3.2.2. WPA

Wi-Fi Protected Access (WPA), WEP'in zayıflıklarını gidermek amacıyla 2004 Wi-Fi Alliance tarafından geliştirilmiştir. WEP'in güvenliğini tamamen yitirmesi üzerine IEEE, 802.11i adını verdiği yeni bir güvenlik mekanizması geliştirme çalışmalarına başlamıştır. Bu geçiş sürecinde güvenliğin sağlanması, geçici bir süreliğine olsa da WPA tarafından gerçeklenmektedir. Bunun nedeni ise; WPA'nın ek bir donanım gerektirmemesi, yazılım veya cihaz yazılım güncellemeleriyle geçişin sağlanabilmesidir.

WPA ile 802.1x tabanlı asıllama yapılması zorunludur. Ancak, bu yöntemde RADIUS sunucusu kullanımı isteğe bağlıdır. Bunun yerine ön-paylaşımlı anahtar (pre-shared key – PSK) kullanımı ile asıllama işlemi yapılabilmektedir. Bir RADIUS sunucusu kullanımı halinde ise WPA tüm 802.1x ve EAP protokollerini desteklemektedir. WPA, şifreleme mekanizması olarak, yine kendine has ve geçiş sürecindeki ihtiyaçları karşılamayı hedefleyen farklı bir protokolü kullanmaktadır. TKIP (Temporal Key Integrity Protocol) adı verilen bu protokol WEP'te olduğu gibi RC4 algoritmasını kullanır. Fakat geliştirdiği yeni yöntemlerle WEP'in zayıflıklarını çok büyük ölçüde gidermiştir.

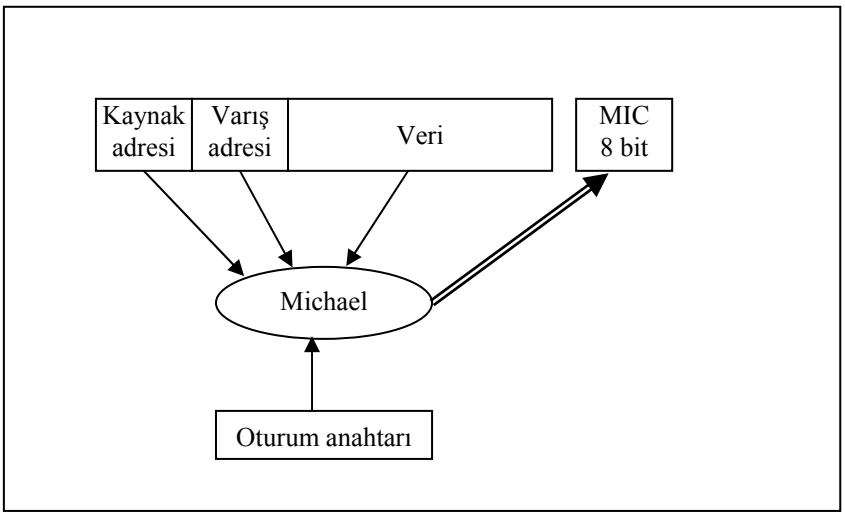
TKIP ile IV 48 bite çıkarılmıştır. IV hem paketlere sıra numarası vermede hem de her paket için yeni bir anahtar oluşturmada kullanılır. Paketlere sıra numarası verilmesinin amacı tekrar saldırılarını engellemek içindir. Bu şekilde sırasız gelen

paketler alıcı tarafından kabul edilmeyecektir. Her paket için ayrı ayrı oluşturulan anahtarın 48 bit ile tekrarlanma sıklığı yaklaşık 100 yıldır. Dolayısıyla WEP'e kıyasla çok daha güvenli anahtarlar üretilmektedir. Bu şekilde tekrar eden IV'lerin dinlenerek anahtarın ele geçirilmesi çok güçtür. Tekrar saldırılarına karşı WPA da TSC (TKIP Sequence Counter) kullanılır. TSC esasen IV ile aynı şeydir. TSC ile tekrar saldırılarını önlemenin prensibi; gelen paketin sıra numarası, bir önce gelen paketten 1 fazla değilse, o paketi reddetmesidir. TSC, oturum anahtarından oluşturulan geçici şifreleme anahtarı ve MAC adresi kullanılarak her paket için ayrı bir şifreleme anahtarı üretilir. Paketlerin şifrelenmesi için farklı anahtarlar oluşturulması Şekil 4.8'de gösterilmiştir.



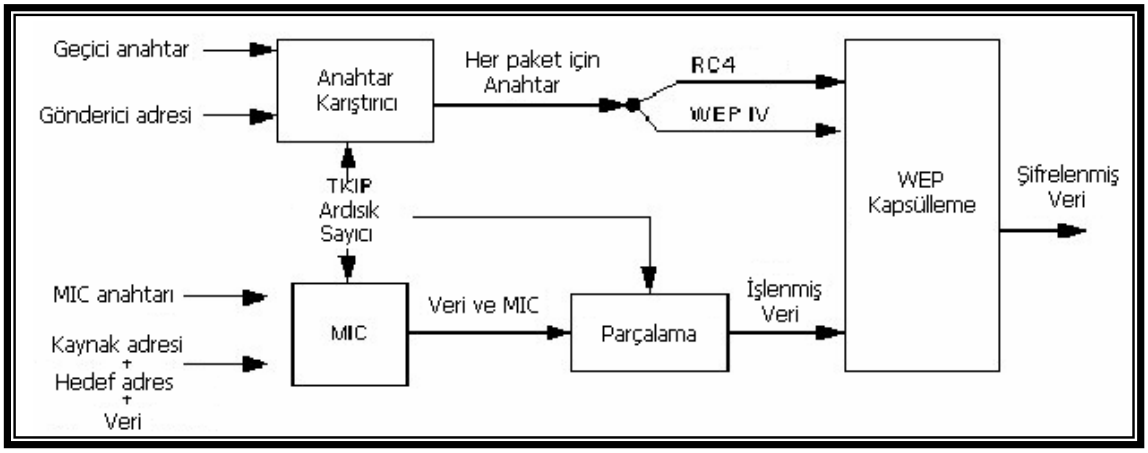
Şekil 4.8. Farklı şifreleme anahtarı oluşturulması

TKIP'de veri bütünlüğünü sağlamak için Michael algoritması kullanılır. Michael veri bütünlük kodu (MIC- Message Integrity Code) alıcı ve verici MAC adreslerini alarak sağlama bitleri (checksum) oluşturur. Bu bitler verinin sonuna şifrelenerek eklenir. Şifreleme, mesaj içeriğinin saldırgan tarafından değiştirilmesini önler. Ayrıca MAC adresleri de WEP'te olduğu gibi açık bir şekilde gönderilmez. Michael algoritmasına girdi olarak MAC adreslerinin yanı sıra oturum anahtarı ve veri paketi de girer. Sonuç olarak 8 bitlik sağlama verisi oluşturulur. Şekil 4.9 sağlama bitlerinin oluşturulmasını göstermektedir [23,25,27,28].



Şekil 4.9. MIC kodunun elde edilmesi

TKIP'de verinin şifrelenerek gönderim aşamaları Şekil 4.10'da gösterilmiştir. Elde edilen bu veri EAP mekanizması ile ağ trafiğine sokulur.



Şekil 4.10. TKIP ile verinin gönderilme aşamaları

WEP'te kullanılan anahtar statik bir anahtar olmakla birlikte gerek asıllama gerek şifreleme mekanizmasında tek başına kullanılıyor olması WEP'in en büyük güvenlik açığı olarak değerlendirilmektedir. WPA'da getirilen güçlü asıllama ve şifreleme mekanizmaları (802.1x, TKIP) kablosuz ağlardaki güvenlik sorununu büyük ölçüde çözmüştür. Ancak WPA'nın da WEP ve dolayısıyla RC4 tabanlı bir güvenlik mekanizması olması, güvenilebilirliğini azaltmaktadır. Nitekim WPA'ya karşı

yapılan bazı saldırıların başarılı sonuç verdiği bilinmektedir. Yine de WPA WEP'e oranla çok daha güvenilir bir teknoloji sunmaktadır. WEP ve WPA'nın bir karşılaştırması Tablo 4.1'de verilmiştir.

Tablo 4.1. WEP ve WPA'nın karşılaştırılması

WEP	WPA
Ön paylaşımlı anahtar mekanizması ile güvenliği sağlar. Anahtar kullanıcılar arasında ortaktır.	802.1x asıllama ile kullanıcıya has anahtar üretilir.
Kullanılan senkron akış şifreleme ağ ortamları için uygun (güvenli) değildir.	WEP ile aynıdır.
Her paket için IV tarafından üretilen anahtar zayıf bir anahtardır ve saldırılara karşı açıktır.	Ortak anahtar kullanılarak üretilen geçici şifreleme anahtarı ve anahtar karıştırıcı fonksiyonları ile kırılması güç anahtarlar her paket için ayrı ayrı oluşturulur.
Statik anahtar + küçük boyutlu IV + her paket için anahtar üretim metodu = İstenilen güvenliği sağlamak için yeterli değildir.	48 bit IV + her oturum için yeniden anahtar üretilmesi = Daha güvenli bir sistemdir.
IV'lerin tekrarlanma olasılığı çok yüksektir.	IV'lerin tekrarlanma olasılığı çok düşüktür.
Veri bütünlüğü için doğrusal bir algoritma kullanır. Bu zayıf bir veri bütünlüğü korumasıdır.	Veri bütünlüğü için doğrusal olmayan Michael algoritması kullanır. Bu güçlü bir veri bütünlüğü korumasıdır.
Alıcı ve gönderici adresleri şifrelenmeden gönderildiği için veri farklı adreslere yönlendirilebilir.	Alıcı ve gönderici adresleri de şifrelenir.
Tekrar saldırılarına karşı korumasızdır.	Ardışık sayı üretici ile tekrar saldırılarına karşı koruma sağlar.
Kullanıcı AP'yi asıllamaz.	802.1x ile karşılıklı asıllama yapılır.

4.3.2.3. IEEE 802.11i (WPA2)

IEEE 802.11i, RSN (Robust Security Network) adında yeni bir kablosuz ağ türü tanımlar. Bu bazı durumlarda WEP tabanlı ağlarla aynıdır fakat bununla birlikte RSN'e bağlanmak için kablosuz cihazların RSN uyumlu olması gerekir. RSN uyumlu cihazlar yazılım güncellemesi ile elde edilememektedir. Ancak üretim aşamasında bu sağlanabilir. Bu yüzden yazılım güncellemesi ile kullanılabilen WPA teknolojisinden farklı olarak WPA2 olarak da adlandırılan 802.11i teknolojisini kullanabilmek için mevcut kablosuz cihazların RSN uyumlu cihazlarla değiştirilmesi şarttır. Bu da günümüzde oldukça yaygın olarak kullanılan kablosuz cihazların değiştirilmesinin yüksek maliyet gereksinimleri dolayısıyla 802.11i teknolojisinin genellikle kullanılmadığını göstermektedir. Bununla birlikte 802.11i ile kablosuz ağlarda tam bir güvenlik sağlanmaktadır.

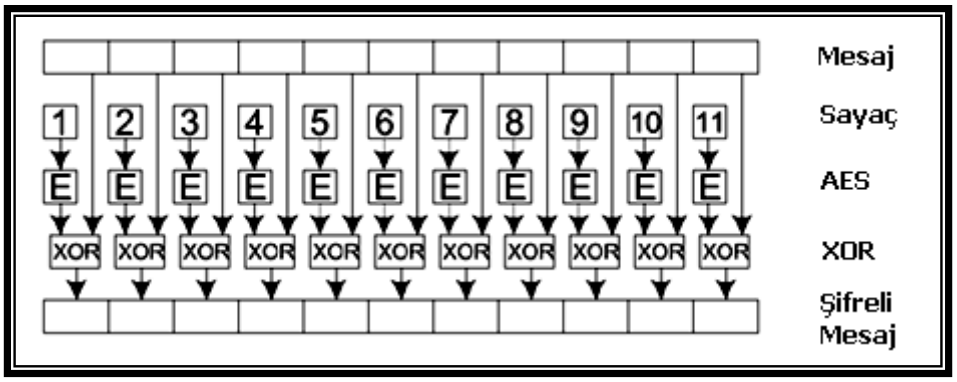
WPA2'de kullanılan yöntemler genel hatlarıyla WPA'da kullanılanlarla aynıdır. WPA2'yi WPA'dan farklı kılan tek özellik ise şifreleme algoritmasında ortaya çıkmaktadır. Asıllama ve anahtar üretme mekanizmaları WPA ve WPA2'de aynıdır. Ancak RC4 şifreleme algoritmasından kaynaklanan zayıflıkları gidermek amacıyla, WPA2 farklı bir şifreleme algoritması kullanmaktadır. AES (Advanced Encryption Standard) adı verilen bu algoritma ile gerçekleştirilen şifreleme günümüzde tam bir güvenlik sunmaktadır. Bilindiği üzere RC4 algoritması akış şifreleme tekniğini kullanmaktaydı. AES algoritmasında ise güçlü blok şifreleme tekniği kullanılmaktadır. AES algoritması NIST (National Institute of Standards and Technology) tarafından 2002 yılında geliştirilmiştir.

WPA2'de güvenlik AES şifreleme algoritmasını kullanan CCMP (Counter Mode – CBC MAC Protocol) protokolü ile sağlanır.

Counter Mode:

Counter Mode kullanımında bir sayaca gereksinim vardır. Sayaç, keyfi fakat önceden belirlenmiş bir değerle, belirlenmiş bir usulde artmaya başlar. Örneğin, sayaç 1 değerinden başlar ve her blok için 1 artar. Birbirini takip eden her bir mesaj için o

anki değerden sayacın başlangıç değeri türetilir. AES şifreleme, sayaç bir anahtar akışı ile şifrelendikten sonra yapılır. Daha sonra üretilen 128 bitlik bu blokla, 128 bitlik bloklara ayrılmış veri XOR işlemine tabi tutulur. Sayaç değeri aynı anahtar ile tekrarlanmadıkça sistem güvenlidir. WPA2'de her oturum için yeni bir anahtar kullanımı ile bu başarılmaktadır. Counter Mode ile şifreleme işlemi matematiksel olarak Ci = Mi (XOR) Ei şeklinde ifade edilebilir. Burada i sayaç, E AES şifresi, M mesaj, C şifreli mesajdır. Counter Mode ile şifreleme Şekil 4.11'de gösterilmiştir.



Şekil 4.11. Counter Mode ile şifreleme [25]

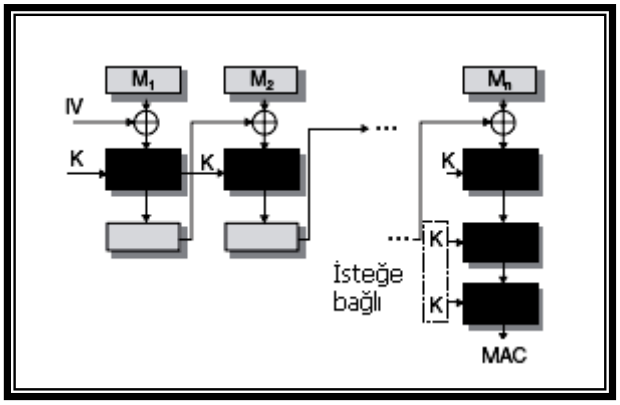
Counter Mode'un özellikleri şöyle sıralanabilir:

- Akış şifreleme tarafından işlenmiş olan blok şifrelemeye izin verir.
- Counter Mode, mesajdan bağımsız ve mesaj hedefe ulaşmadan önce oluşturulmuş anahtar akışına izin verir.
- Mesajın farklı bloklarının şifrelenmesi arasında bir ilişki yoktur; mesajın farklı blokları donanımsal bir AES mekanizması tarafından paralel olarak şifrelenir.
- Şifreyi çözme işlemi şifreleme ile tamamen aynıdır. Çünkü XOR işlemi iki defa tekrarlanırsa aynı veriye ulaşılır. Burada, şifrenin çözülmesi için AES bloklarının bilinmesi yeterlidir.

Counter Mode sadece veri gizliliğini sağlar, veri bütünlüğünü sağlamaz. 802.11i çalışma grubu veri bütünlüğünü sağlamak için Cipher Block Chaining (CBC)-MAC işlemini kullanır. CBC, bir mesaj bütünlük kodu (MIC) üretir. MIC şifrelenmiş bir mesaj asıllama kodu oluşturur.

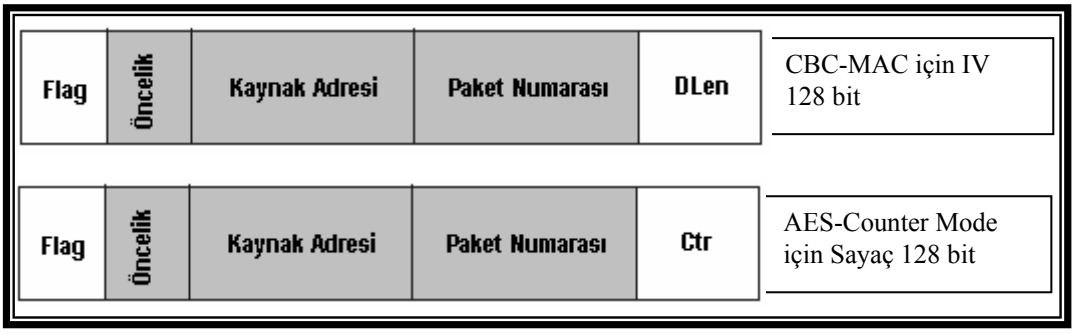
CBC-MAC işlemi şu şekilde yapılır:

1. Mesajın ilk bloğu alınır IV ile XOR işlemine tabi tutulur ve bir anahtar ile AES kullanılarak şifrelenir.
2. Sonuç, ikinci blok ile XOR işlemine tabi tutulur ve sonra elde edilen sonuç şifrelenir.
3. Elde edilen bu sonuç da, takip eden blokla XOR işlemine tabi tutulur; sonuç şifrelenir. Bu işlem son blok kullanılana kadar devam eder. Sonuç olarak tek blok uzunluğunda şifrelenmiş bir veri oluşur.



Şekil 4.12. CBC ile veri bütünlüğü [28]

IV ve sayaç paketleri 128 bit uzunluğundadır ve Şekil 4.13'de gösterilmiştir.

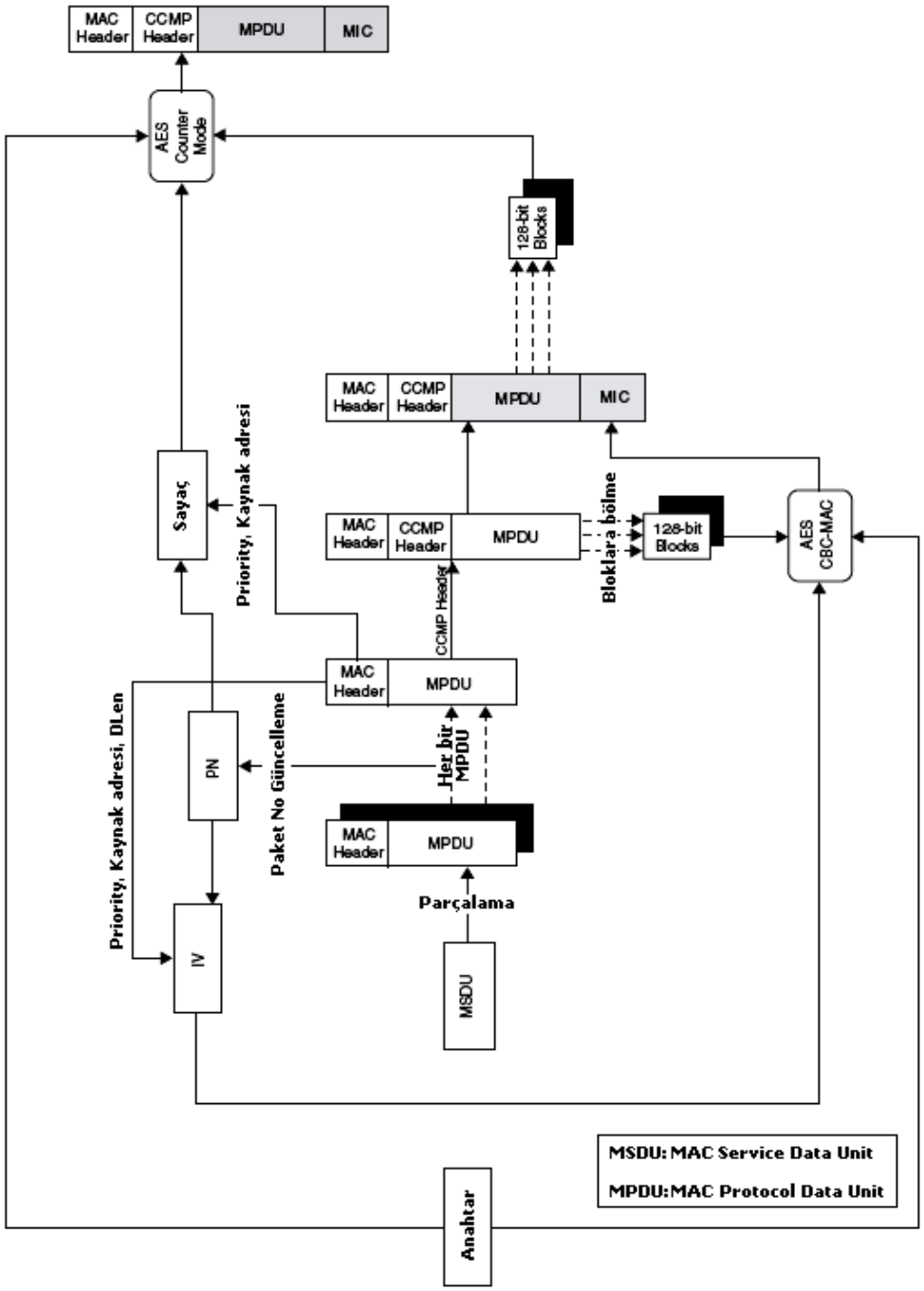


Şekil 4.13. Sayaç ve IV veri paketleri [28]

Burada flag sabit ikili bir değerdir. Öncelik biti gelecekteki kullanım için ayrılmıştır. DLen, şifrelenmemiş verinin boyutunu, Ctr ise sayaç başlangıç değeri bilgisini tutar.

WPA2'de şifreleme işlemi Counter Mode ve CBC-MAC kullanılarak gerçekleştirilir. Bu iki yöntemin hepsine birden CCMP (Counter Mode CBC-MAC Protocol) adı verilir. Verinin CCMP ile tamamlanmış şifreleme işlemi Şekil 4.14'de gösterilmiştir.

WPA2 kablosuz ağlarda dolaşım (roaming) da sağlar. Kullanıcı bir AP'ye bağlı iken diğer bir AP'yi algılarsa 802.1x anahtar değişimi ile yeni AP için anahtarları da elde eder ve saklar. Ya da AP ile daha önceden anahtar belirlenmiş ise bu anahtarlar bellekte saklanarak, bu AP ile iletime geçildiğinde 802.1x işlemlerini tekrar yapmaya gerek kalmaz. Ayrıca 802.11i güvenlik standardı 802.11e servis kalitesi (QoS) standardı ile uyumludur [25,28].



Şekil 4.14. WPA2 şifreleme mekanizması [28]

4.3.2.4. Sanal özel ağ ile güvenlik

Kablosuz ağlarda güvenliği sağlamak için, özellikle veri gizliliğinin çok önemli olduğu şirket ve kuruluşlarda sanal özel ağ (VPN – Virtual Private Network) oluşturulmaktadır. VPN, genel erişimli ağların içinde gizli iletişimi sağlamak için

şifrelenmiş kanallar, asıllama mekanizması ve erişim kontrolü seçenekleri sunar. VPN'in bazı özellikleri:

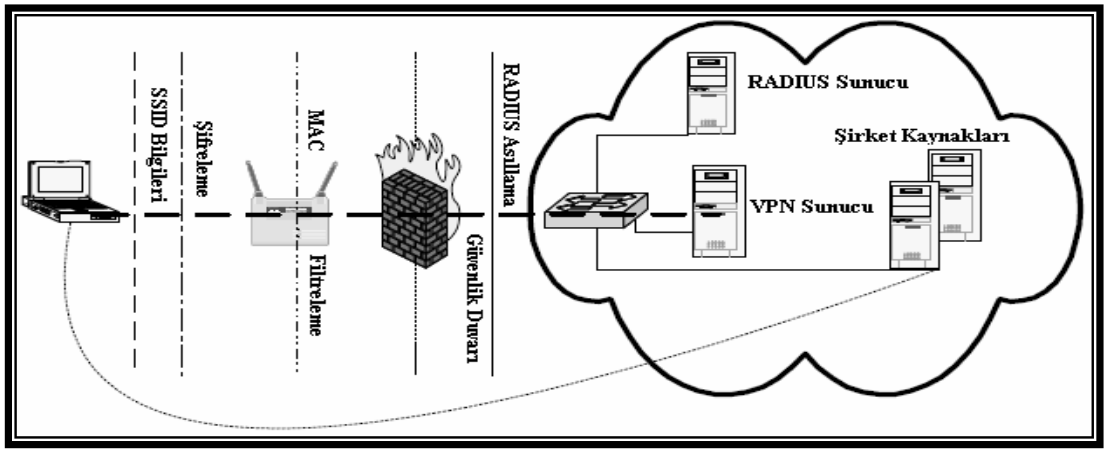
- İki nokta veya iki ağ arasında şifreli iletişim sağlar.
- Genellikle yazılım tabanlıdır. (Donanım tabanlı da olabilir.)
- Dış kısıtlamaları sağlayan değişken şifreleme katmanları sunar.

VPN'in faydaları:

- Ofis içindeki iletişimi ve güvenliği kolaylaştırır.
- Gezgin kullanıcılar için ucuz ağ erişimi sağlar.
- Farklı bir yerde olunsa da şirket ağına tam bir erişim sağlar.

Tünelleme (tunneling) tekniği ile veri paketleri diğer veri paketlerinden güvenli bir şekilde ayrılır. IPSec (Internet Protocol Security) VPN için asıllama ve şifreleme mekanizmalarını oluşturur. Ayrıca VPN ile ağda her anlamıyla tam bir merkezi yönetim sağlanmış olur. Ancak VPN karmaşık bir yapıya sahiptir ve kurulması ve yönetilmesi ancak uzman personel tarafından yapılabilmektedir [17,29].

Kablosuz ağlarda VPN kullanımı Şekil 4.15'te gösterilmiştir.



Şekil 4.15.WLAN'da VPN kullanımı [17]

4.3.2.5. Diğer Güvenlik Önlemleri

WPA henüz geliştirilmemişken, WEP'in açıklarını kapatabilmek amacıyla bazı yöntemler denenmiştir. AP, kimliğini (SSID) yayın yaptığı frekans aralığında şifresiz olarak yayınlar. Kapsama alanı içinde bulunan bir kablosuz istemci, yayınlanan bu kimliği algılar. Eğer o AP'ye üye ise kablosuz ağa bağlantı sağlar. Bu noktada, 802.11 standardında tanımlı olmamakla birlikte, bazı üreticiler AP'lerinde SSID yayınlama özelliğini devre dışı bırakma seçeneğini sunarlar. Bu şekilde, AP'nin kimlik bilgilerine sahip olmayan bir kullanıcının (saldırgan) ağa erişimini engellemeye dolayısıyla güvenli bir bağlantı sunmaya çalışırlar. Ancak bu yöntem başarılı olamamıştır. Bazı pasif dinleme yazılımları ile ortamdaki iletişim dinlenerek, kimliği gizlenmiş AP'ler kolaylıkla tespit edilmektedir.

Diğer bir güvenlik önlemi ise; yine 802.11 standardında tanımlı olmayan MAC filtreleme yöntemidir. Bu yöntemde AP, sadece önceden tanımlanmış MAC bilgisine sahip cihazlardan gelecek istemleri kabul etmektedir. Tanımlama listesinde bulunmayan bir cihaz –bu genellikle ağa üye olmayan bir kullanıcıya aittir- ortak anahtara sahip olsa bile ağa bağlanamayacaktır. Bu yöntem de hedeflediği güvenlik kriterlerini sağlayamamıştır. Ağdaki trafik dinlenerek AP'de tanımlı cihazların MAC bilgileri elde edilmektedir. Çünkü WEP'te MAC bilgileri şifrelenmeden gönderilmektedir. Daha sonra elde edilen bu kayıtlı MAC bilgileri, saldırgan tarafından kendi MAC bilgileri ile değiştirilmekte ve böylelikle AP, üye olmadığı halde yabancı bir kullanıcıya erişim sunmaktadır.

4.4. Ağı Tehlikelerden Korumak

4.4.1. WLAN güvenlik açıkları

Zayıflıklar sistemin tasarımı sırasında gözden kaçan, kötü tasarlanan sistemlerde bulunan veya sistem tasarımının bir parçası olan donanım veya yazılım kusurlarıdır ki bu kusurlar sistemin işleyişini etkileyebilir veya istismar edilmesine olanak verebilirler. Bu olası istismarlar veya işleyiş bozuklukları sistemin teklemesi, arıza

çıkarması şeklinde veya yetkisiz girişlere olanak sağlaması, sistemin koruduğu bilgilere veya bir kısmına izinsiz erişim hakkı tanıması şeklinde olabilir.

1990 öncesi bu zayıflıklar bilişim ve ağ teknolojilerinde iyi bilinmiyordu ve genellikle ihmal ediliyorlardı. Ancak bilgisayar ağlarının çok yaygın bir şekilde kullanılmaya başlanması, onun güvenli bir hale getirilmesi ihtiyacını da beraberinde getirmiş ve zayıflıkların giderilmesi için bilimsel çalışmalara büyük maddi kaynaklar ayrılmıştır.

Kablolu ağlarda zayıflıklar:

Kablolu ağlarda veri paketleri göndericiden alıcıya teller aracılığı ile switch (anahtar), router (yönlendirici) ve gateway (ağ geçidi) üzerinden iletilmektedir. Ağa bu donanımlar üzerinden fiziksel bir bağlantı kurabilen herhangi biri veri paketlerini toplayabilir, inceleyebilir, okuyabilir ve daha fazla olarak da bu verileri bozabilir veya silebilir. Kablolu ağlardaki bu zayıflıkları sınıflandırırsak:

Paket izleme: Ağdaki herhangi iki veya daha çok bilgisayar birbirleri ile iletişim kurarken birbirlerine yolladıkları paketler okunabilir, analiz edilebilir veya düşürülebilir. Bu yöntemde yol alan paketler şifrelenmemiş iseler tam anlamıyla saldırıya açıktırlar. Eğer paketler şifrelenmiş ise de sadece iletişim kurulan alıcı tespit edilebilir ve aralarında ne kadar veri transferi yapıldığı, sıklığı tespit edilebilir.

Ortadaki adam (Man In The Middle- MITM): Bu yöntemde saldırgan değişik yollardan birini kullanarak saldırdığı bilgisayardan gönderilen tüm paketleri kendisine yönlendirir ve kendisinden gelen paketleri veya cevap paketlerini dışarıdan geliyormuş gibi gösterir. Örneğin; kurban Microsoft'tan bir güvenlik paketi indirmek istediğinde saldırgan istediği herhangi bir dosyayı mesela virüslü veya sistemi bozan bir dosyayı kullanıcının indirmesini ve çalıştırmasını sağlayabilir.

Servis durdurma (Denial of Service-DoS): DoS saldırıları birden çok paket yollayarak sistemi yavaşlatıp durdurmaya yöneliktir. Bazen bu paketler çok büyük ve içerisinde çalıştırılması istenen kodları içerebilir. Bu paketler ve kodlar sistemin

yükünü arttırmakla beraber sistemin durmasına hatta kilitlenmesine yol açabilir. Genellikle ağ omurgalarında kilitlenmelere sebep olurlar.

Dağıtılmış servis durdurma (Distributed Denial of Service-DDoS): DDoS saldırıları DoS saldırılarının gelişmiş bir türevidir. Bu yöntemde saldırgan girmek istediği bir ağın dışarıya açık bir servisini veya güvenlik duvarını, zombiler kullanarak durdurup, ağa sızmaya olanak hazırlar. Zombiler, trojan veya virüs bulaştırılmış bilgisayar gruplarıdır ki saldırganlarca belli bir amaç için programlanabilir veya uzaktan kullanılabilirler. Zombiler belli bir zamanda önceden belirlenmiş bir sisteme sürekli olarak sahte paket yollamaya başlarlar. Bu, saldırılan sistemde bir yüke sebep olur ve saldırgan için sistemi aşmak için en iyi zamandır. Hem sistem kendisine zamanında ve düzgün cevap vermeyecektir hem de saldırganın izlenmesi, yakalanması daha da zorlaşacaktır. Üstelik bu zombiler değişik omurgalardan bağlı olacakları için saldırılan sisteme daha fazla yük bindirebilirler. Günümüzde en çok kullanılan yöntemlerden biridir.

Değişken taşmaları: Değişken taşmaları teknik anlamda karmaşık saldırıların ve sistem bozucuların (exploit) temelini oluşturur. Basit anlamda saldırgan veri paketlerini anlamsız ve ret edilecek bir biçimde alıcı sisteme yollar. Alınan ve ret edilen bu paketler sistemde normal dışı tepkilere veya işlev bozukluklarına yol açar. Daha geniş anlamda sistem tarafından alınan her bir paket bazı değişkenlere atanır ama akıllıca hazırlanmış bu veri paketleri değişkenlerin bazılarında hatalar oluşmasına sebep olur. Hafızada tutulan bu değişkenler sıralandığında bir kod oluştururlar ki sistemde tutulan bu kodlar yeni bir değişken depolanmak istendiğinde çalışmaya başlar. Daha sonra kartopu etkisi denilen bir yöntemle sistem istenilen kodlar bünyesinde çalışır durumda servis vermeye devam eder. Genellikle arka kapı açmak için kullanılırlar. Bu da sisteme giriş için bilet demektir. Ama iyi bir değişken taşması bulmak bunun için verileri hazırlamak zordur ve ileri derecede kod bilgisi ve programlama bilgisi ister. Günümüzde pek sık olmasalar bile kısmen diğer saldırı tiplerinde de kullanılırlar. Bu yolla yazılan en iyi saldırı MSBlaster'dır

Trojanlar-virüsler-diğer saldırı yazılımları: Tüm bu varyasyonlar basit bir mantıkla işlerler. Çalıştırılabilir kodu içeren dosyayı indir ve çalıştır. Kurbanlar çeşitli

şekillerde e-posta-resim-mp3 dosyası şekline bürünmüş dosyaları indirip çalıştırırlar ve kod sisteme sızmış olur. Genelde çalışan bu kodlar çalıştığı sisteme yetkisiz erişim, istenmeyen e-posta, DoS, DDoS saldırılarında kullanmak için gereklidir.

Kablosuz ağlarda zayıflıklar:

Kablolu ağlarda bulunun tüm zayıflıklar kablosuz ağlarda da bulunmaktadır. Özellikle fiziksel sınırlamalar yüzünden kablolu ağlar kablosuz ağlara göre daha az risklidirler. Kablosuz ağlara has zayıflıklar:

Sahte AP: Bu yöntem basit ama teknik anlamda erişim çalma ve diğer saldırılara ön ayak olmada en etkilisidir. Kablosuz ağın yakınlarına aynı SSID ile başka bir AP kurulur. Ağa bağlanmak isteyen yetkili kullanıcılar, bu sahte AP'ye kullanıcı adı ve şifrelerini bildirecekler ve böylece saldırgan bu bilgileri elde edecektir. Hatta sahte AP herhangi bir şekilde kablosuz ağ dahilinde kurulabilir ve kullanıcılara internet hizmeti de sağlayabilirler. Bu durumda kullanıcılar sahte bir AP'ye bağlandıklarının farkında olmayacaklardır. Saldırgan, bu yöntemde çok kolay bir şekilde MITM saldırılarını gerçekleştirebilir.

Sahte kullanıcılar: Sahte kullanıcılar, kablosuz ağlara diğer kullanıcıları izleyerek, MAC adreslerini alarak, sinyallerini kopyalayarak yetkisiz erişime sahip olabilirler.

Açık AP'ler: Birçok AP fabrika çıkışı herkese açık şeklinde üretilirler. Bu AP'lerden erişim yetkilendirmeleri istenmez. Bu AP'ler sayesinde internet erişimi ve daha önemlisi ağa giren bir kapı elde edilir.
Frekans bozucular: Tüm kablosuz bağlantılarda çeşitli frekanslarda radyo dalgaları kullanılır ki radyo dalgalarının yayılımı ile kablosuz iletişim bozulabilir. Bu basit bir DoS saldırısı sayılabilir ama kablosuz ağlarda frekans bozma çok daha kolaydır. Frekans bozma yasal değildir ama en yaygın kablosuz ağ saldırılarındandır.

Yüksek kazançlı antenler: Düşük güç kablosuz ağlar, kapsama alanı olarak daha güvenli olarak kabul edilirler oysaki bu tamamen yanlıştır. Kablosuz ağlara saldırılar, onun kapsama alanı içinden yapılmaktadır. Dolayısıyla, kapsama alanı dar tutularak

veya kontrol edilebilir bir şekilde tasarlanarak saldırılara karşı önlem alınmaya çalışılabilir. Bu çoğu zaman çok etkili bir yöntemdir ve çok önemli bir güvenlik kriteri olarak kabul edilmektedir. Kötü niyetli bir saldırgan, bu güvenlik önlemini yüksek kazançlı anten kullanarak aşabilir. Şöyle ki; yüksek kazançlı antenler ile çok uzakta bulunan ve kapsama alanı kontrol edilebilecek şekilde tasarlanmış bir kablosuz ağa erişilebilir. Günümüzde yüksek kazançlı antenler ile 15 mil uzaklıktaki radyo dalgaları algılanabilmektedir [30].

4.4.2. WLAN'a yapılan saldırılar

Kablosuz ağlar için geliştirilen farklı güvenlik mekanizmalarına rağmen, onlara saldırı için birçok yol vardır. WEP, WPA ve EAP'ın açıklarından yararlanılarak yapılan saldırılar bilinmektedir. Bu saldırıları gerçekleştiren birçok araç piyasada mevcuttur.

WEP'e yapılan saldırılar:

WEP ile şifrelenmiş kablosuz ağlara karşı yapılan iki tür saldırı yöntemi vardır. Birincisi zayıf IV'lerin toplanmasına; ikincisi ise tekrar etmeyen IV'lerin toplanmasına ihtiyaç duyar.

Zayıf IV kullanımına karşı yapılan saldırılar:

FMS saldırıları olarak bilinen bu tür saldırılar, WEP'in RC4 şifreleme algoritmasını kullanmasından ileri gelen zayıflıkları temel alır. Şifrelenmiş paketler içindeki IV'ler toplanarak WEP anahtarının elde edilmesi şeklinde çalışır. Toplanan IV'ler içinden tekrar edenlerin incelenmesi prensibine dayanır. 5 milyon şifreli paket içinden süzülmüş 3.000 zayıf IV toplanarak WEP anahtarı başarıyla elde edilebilmektedir. Zayıf IV'ler toplandıktan sonra, şifreleme aşamaları ters yönde uygulanarak anahtarın ilk byte'ı elde edilir. Bu işlem WEP anahtarı ele geçirilene kadar her byte için tekrarlanır.

IV'ye karşı vuruş (chopping) saldırıları:

Vuruş saldırıları, yeterli sayıda şifreli paket toplanması esasına dayanır. Vuruş saldırılarının bir yöntemi olarak, tekrar etmeyen IV'ler toplanarak paketin son byte'ı paketten çıkarılır ve anahtar doğru bir şekilde tahmin edilmeye çalışılır. Son byte ICV bitlerini içerir. Son byte 0 olduğunda, paket içindeki son 4 byte ile XOR işlemine tabi tutularak ICV bitleri ele geçirilebilir. Sonra bu paket tekrar gönderilerek şifresi kırılır.

WEP'e karşı yapılan saldırılar için en büyük problem yeteri sayıda paketin toplanabilmesi için haftalarca hatta aylarca zaman geçmesinin gerekebileceğidir. Ancak bu işlemi hızlandırmak mümkündür. Bunun için AP'ye çok sayıda paket gönderilebilir. Gönderilen bu paketler ARP (Address Resolution Protocol) paketleridir ve asıllama işlemini başlatmada kullanılır. Bu şekilde ağda bir trafik oluşturulacak ve paketler hızlı bir şekilde toplanacaktır. İlk ARP paketlerinin tekrar tekrar gönderilmesi problem yaratabilir. Bunu engellemek için asıllama sırasında sahte ARP paketleri üretip ağda istenen trafiği sağlayan araçlar mevcuttur. Bu; üye kullanıcılarla AP arasındaki asıllama işlemi sırasında ağ dinlenerek, yeterli sayıda ARP paketi toplayarak gerçekleştirilir.

WPA'ya yapılan saldırılar:

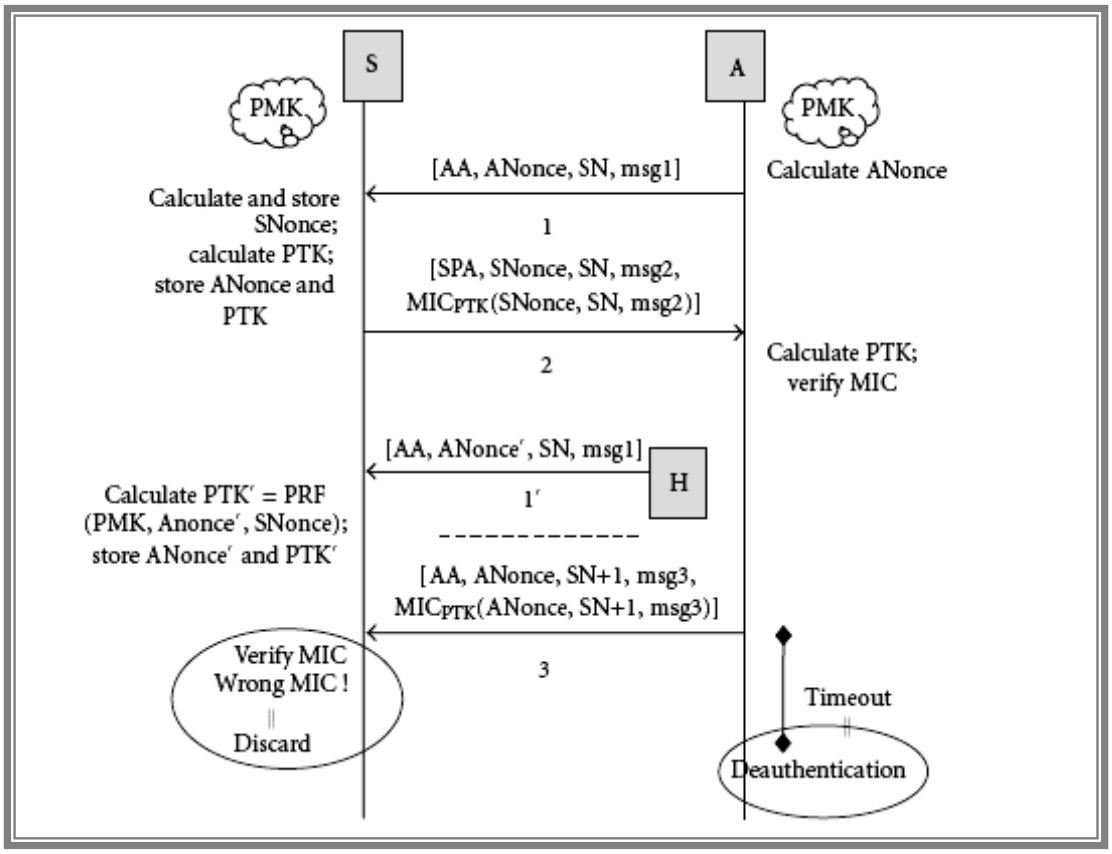
WPA'ya yapılan saldırılarda WEP'te olduğu gibi çok sayıda paket toplamaya ihtiyaç yoktur. Önemli bir nokta da; WPA'ya karşı yapılan saldırıların başarılı olması için WPA'nın ön paylaşımlı anahtar (PSK) modunda çalışıyor olması gerektiğidir. WPA-PSK'ya karşı başarılı bir saldırı gerçekleştirmek için EAPOL mesajlarını (dörtlü anlaşma mesajları) yakalamak gerekir. Bu mesajları yakalamak için yetkili bir asıllama işleminin yapılması beklenebilir ya da asıllanmamış paketleri AP'ye bağlanmış istemcilere göndererek yeni bir asıllama işlemi için zorlanabilir. Yeniden asıllama yapılırken de EAPOL mesajları yakalanabilir. Sonra, her bir anahtar sözlüğü; 4.096 HMACSHA1 (Hashed Message Authentication Code-Secure Hash Algorithm 1) yinelemesi ve kullanıcı-asıllayıcı MAC bilgileri ile birlikte harmanlanmalıdır. Bu tür saldırıların başarılı olması ihtimallere bağlıdır ve başarı için PSK anahtarının 21 karakterden az olması gerekir. Ancak bazı anahtar sözlükleri

ile bu sınır genişletilebilir. Bu tür anahtar sözlükleri piyasada ücretsiz olarak temin edilebilmektedir.

Dörtlü anlaşma (Handshake) protokolüne yapılan DoS ve DoS taşma saldırıları:

Dörtlü anlaşma protokolünün zayıflığı Msg1 mesajından kaynaklanmaktadır. Çünkü bu mesaj veri bütünlüğünü sağlayacak olan MIC değerini içermez. Asıllayıcıdan kullanıcıya gönderilen Msg1 mesajı, saldırgan tarafından elde edilerek ANonce, SN ve mesaj tipi bilgileri belirlenebilir. Saldırgan (H), Msg2 mesajı gönderildikten sonra araya girerek Msg1 mesajına benzer bir mesajı ($Msg1^{l}$) kullanıcıya tekrar gönderir. Bu yeni $Msg1^{l}$ değeri Msg1 değerinden sadece ANonce değeri bakımından farklıdır. Çünkü ANonce değeri rastgele üretilen bir değerdir. Bu noktada kullanıcı, saldırgan tarafından gönderilen bu yeni mesaja tepki olarak yeni bir PTK değeri (PTK^{l}) hesaplayacak ve yine bununla ilişkili olan $Msg2^{l}$ mesajını asıllayıcıya gönderecektir. Asıllayıcı $Msg2^{l}$ mesajını dikkate almayacak ve Msg3 mesajını kullanıcıya gönderecektir. Bu noktada kullanıcı, en son hesapladığı PTK^{l} değeri ile Msg3 mesajını denetleyeceği için ve bu işlem sonucunda bir eşitlik sağlanamayacağı için Msg3 mesajını reddedecektir. Belli bir zaman sonunda asıllayıcı Msg4 mesajını alamadığı için Msg3 mesajını tekrar göndermeyi deneyecektir. Ancak cevap alması mümkün değildir ve belli bir deneme sonunda asıllama işlemi iptal edilecektir. Bu durum Şekil 4.16 ‘da gösterilmektedir.

Kullanıcı her bir Msg1 mesajını aldıktan sonra ANonce ve PTK değerlerini saklamaktadır. Saldırgan DoS Taşma saldırıları ile çok sayıda saldırıda bulunduğunda kullanıcı çok sayıda ANonce ve PTK değerini saklamak zorunda kalacak ve bu da kullanıcı tarafında bellek yorulmasına ve kilitlenmelere sebep olacaktır.

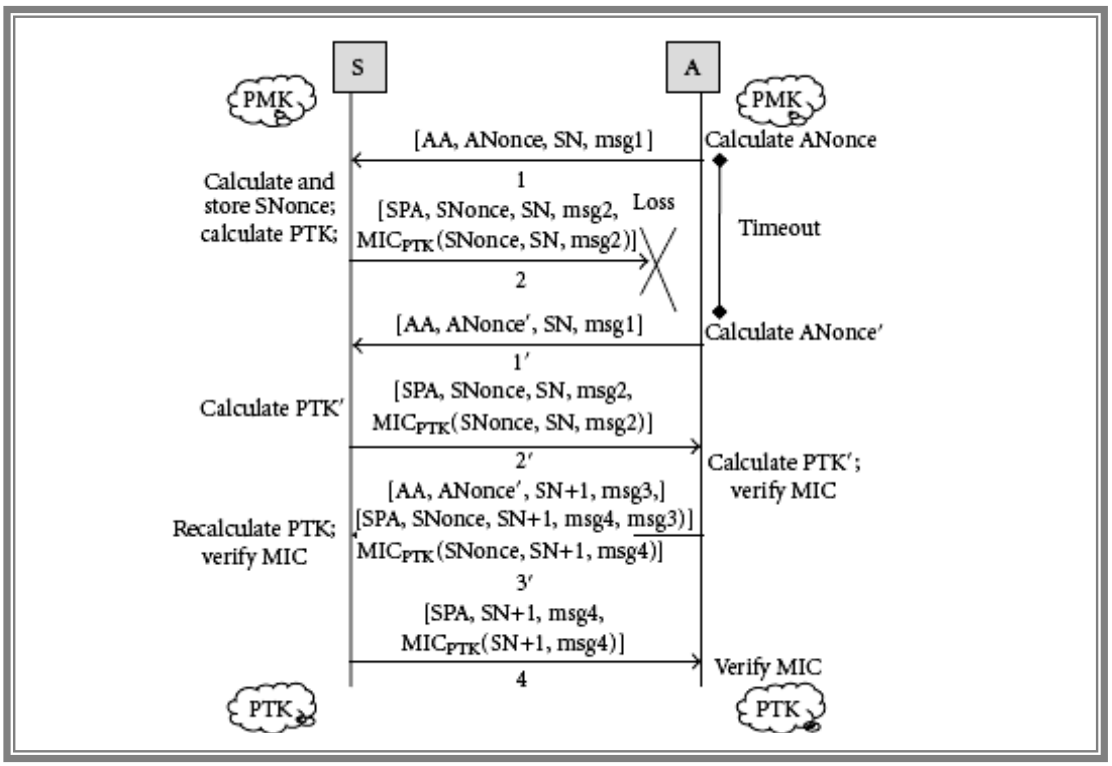


Şekil 4.16. Dörtlü anlaşmaya karşı DoS saldırısı [31]

WPA2 standardı ile bu saldırılara karşı önlemler alınmıştır. WPA2 ile Msg1 mesajı içine PMKID adı verilen yeni bir alan eklenir. PMKID değeri, PMK, AA ve SPA değerlerinin 128 bit SHA harmanlama (hash) fonksiyonu ile elde edilmektedir. Saldırgan PMK değerini bilmediği ve SHA fonksiyonunu tersine çeviremeyeceği için Msg1 mesajını kullanıcıya gönderemez. Bu şekilde WPA2 ile DoS saldırıları engellenmiş olur.

WPA2 ayrıca bellek yorgunluğu problemine de çözüm getirmiştir. Bu çözüm gereği kullanıcı şu şekilde davranmaktadır: Msg1 mesajını aldıktan sonra SNonce değerini üretir, PTK değerini hesaplar ve Msg2 mesajını asıllayıcıya gönderir. Fakat ANonce ve PTK değerlerini saklamaz. Bunun yerine sadece SNonce değerini saklar. Her bir yeni Msg1 mesajını aldığında ise yeni bir PTK değeri hesaplar. Msg3 mesajını aldıktan sonra da yine bu mesajla gelen ANonce değeri ve daha önceden saklamış olduğu SNonce değerini kullanarak PTK değerini hesaplar. Hesaplanan bu PTK değeri ile MIC değeri kontrol edilir ve asıllama işlemi tamamlanır. Bu uygulama

sayesinde Msg2 mesajı kayıp olsa dahi asıllama işlemi tamamlanabilmektedir. Şöyle ki; Msg2 kaybolduktan belli bir süre sonra, asıllayıcı yeni bir Msg1 mesajını ($Msg1^{l}$) yeni bir ANonce değeri ($ANonce^{l}$) ile birlikte kullanıcıya gönderir. Bu izin verilen bir durumdur ve kullanıcı tarafından kabul edilecektir. Şekil 4.17'de bu asıllama işlemi gösterilmiştir.



Şekil 4.17. WPA2 ile DoS saldırılarından korunma ve asıllama işleminin yapılması [31]

LEAP'e karşı saldırılar:

LEAP kablosuz ağlarda güvenliğin sağlanması için Cisco tarafından geliştirilen 802.1x tabanlı EAP-asıllama protokolüdür. Ne yazık ki, LEAP da, WPA'ya karşı yapılan saldırılara benzer saldırılara açıktır. LEAP, Microsoft tarafından geliştirilmiş MS-CHAPv2 (Microsoft Challenge Handshake Protocol version 2) EAP tabanlı asıllama mekanizmasını kullanır. MS-CHAPv2 zayıf bir veri şifreleme standardı (DES) kullanır ve kullanıcı adı ve şifre ile asıllama işlemini yapar. Asıllama esnasında dinleme yoluyla yakalanan LEAP istek ve cevap paketlerinin son iki byte'ı; daha önceden bir anahtar sözlüğünden üretilmiş olması gereken muhtemel

asıllama bilgileri kombinasyonu ile karşılaştırılır. Üretilen veri ile yakalanan veri aynı olduğunda, kullanıcının kullanıcı adı ve şifresi elde edilmiş olur.

VPN'e yapılan saldırılar:

VPN kullanan kablosuz ağlara saldırı yapmak, mevcut şifreleme standartlarına yapılan saldırılardan çok daha güçtür. Daha doğrusu VPN'e yapılan saldırılar, kablosuz bir saldırı değil kablosuz ağ kullanan ağ kaynaklarına yapılan bir saldırıdır.

Kablosuz ağlar birçok güvenlik açığıyla karşı karşıya kalmışlar ve bazı kuruluşlar bu açıkları kapatmak için farklı çözümler bulmuşlardır. Örneğin; AP'ler iç ağın dışına kurulmuşlar ve iç ağ için bir VPN tüneli oluşturulmadıkça, dahili ve harici tüm ağ kaynaklarına erişimleri engellenmiştir. Bu genellikle bir güvenlik mekanizması kullanılmayan kablosuz ağlarda uygun bir çözümdür. Bu tür kablosuz ağlar esasen açık ağlardır fakat bu ağlara erişim sağlanamaz.

Ne yazık ki, bu durum iç ağa saldırılara sebep olmaktadır. Bu tür ağlara başarılı bir saldırı gerçekleştirmek için ağ ile ilgili her şeyi bilmeye gerek yoktur. Kablosuz ağı kullanan bilgisayarlar genellikle dizüstü (gezgin) bilgisayarlardır. Dizüstü bilgisayarlar iç ağın dışındayken incelenebilir ve iç ağa erişim bilgileri elde edilebilir. Saldırgan, bu bilgisayardan elde ettiği bilgilerle; kullanıcı iç ağa bağlantı sağladığında onu kullanarak kablosuz ağa saldırılarda bulunabilir. Saldırgan, keystroke logger adı verilen tuş darbelerini kaydeden casus bir yazılımı dizüstü bilgisayara yükleyerek VPN asıllama bilgilerini elde edebilir. Bu saldırı, sadece çift-etkili asıllama yöntemi kullanıldığında başarılı olabilir. Bu yönteme örnek olarak, Cisco'nun kullandığı grup şifresi-kullanıcı adı ve kullanıcı şifresi-kullanıcı adı gerektiren ve bunları profil dosyalarında saklayan sistemler gösterilebilir. Bu tür saldırılar, çift etkili asıllama olmayan veya tek kullanımlık şifreler ile yapılan ikincil asıllama mekanizmalarında başarı sağlayamamaktadır [24,31,32,33].

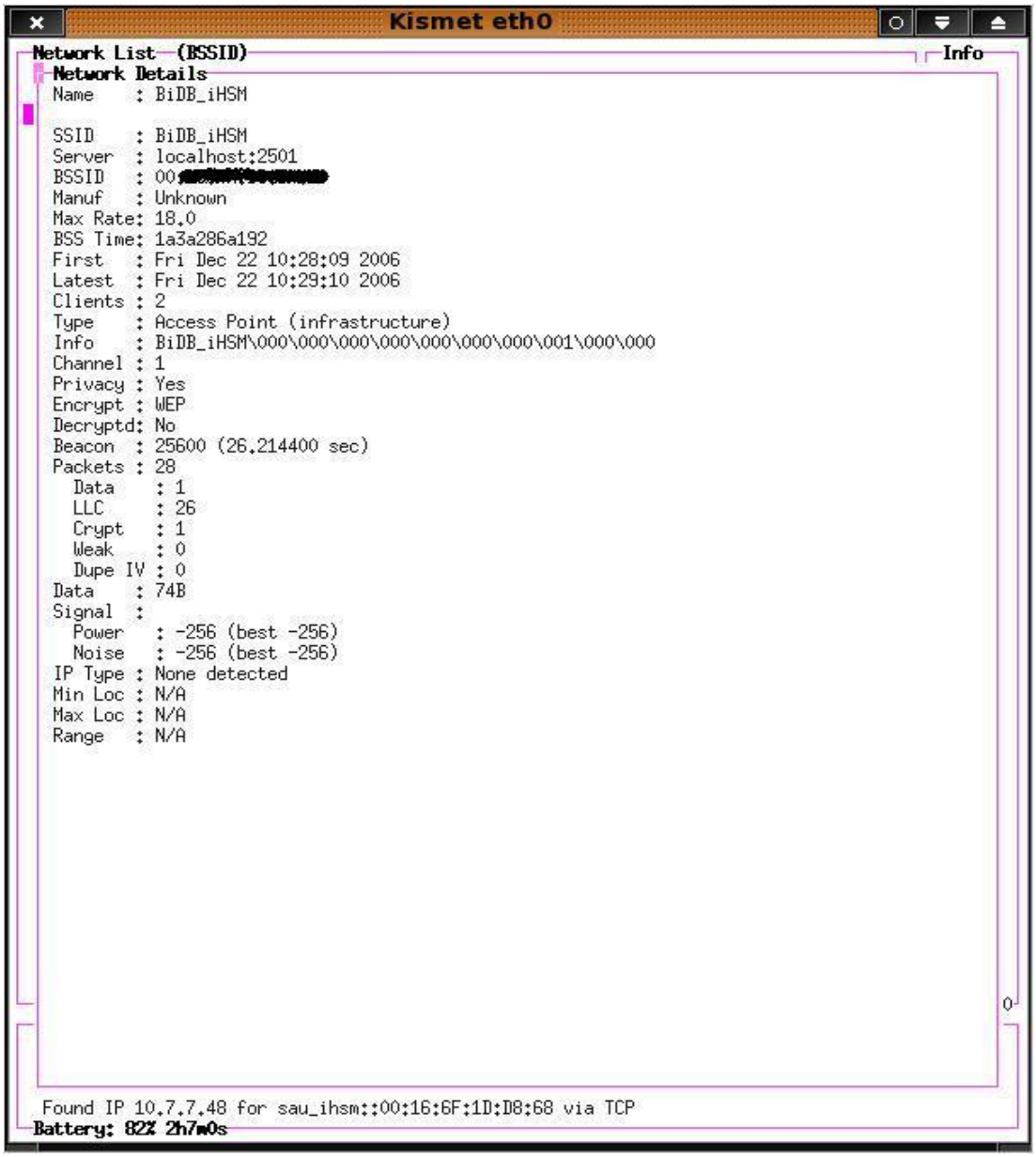
BÖLÜM 5. UYGULAMALAR

5.1. Uygulama 1

Bu tez çalışması kapsamında gerçekleştirilen birinci uygulama iki farklı kablosuz ağ üzerinde yapılmıştır. Birincisi; Sakarya Üniversitesi bünyesinde kurulu olan mevcut kablosuz bir ağdır. Bu ağ bir güvenlik duvarı tarafından korunmaktadır. İkincisi ise orta ölçekli şirketler için örnek teşkil etmesi bakımından başka hiçbir kablosuz ağın olmadığı bir ortamda kurulmuştur. Uygulamaların bu tür iki ağ üzerinde yapılmasının amacı, kablosuz ağların hem profesyonel hem de amatör kullanım durumlarında güvenlik sorunlarının iyice anlaşılmasını sağlamak içindir.

Birinci ağ Cisco AiroNet 1100 AP kullanmaktadır ve kablolu ağa olan bağlantı güvenlik duvarı tarafından engellenmektedir. İkinci ağ ise USRobotics Maxg Router AP kullanmaktadır. Saldırı amaçlı kullanılan bilgisayar Intel pro2200 802.11b/g wireless adapter'e sahip dizüstü bilgisayardır. Uygulamalar sırasında Linux işletim sistemi kullanılmıştır.

Her iki ağ için yapılan saldırılarda, öncelikle ağı tespit edip, veri trafiğini izleyen uygulamalar kullanılmıştır. Kullanılan dinleme/izleme programı "Kismet" programıdır. "Kismet" ile AP'nin adı (SSID), MAC adresi, kullandığı şifreleme mekanizması, yayın yaptığı kanal, bağlı olan kullanıcıların MAC adresi ve iletilen veri paketleri hakkında bazı bilgiler sağlanmaktadır. Bunun yanında "Kismet", SSID yayını yapmayan AP'leri de tespit edebilmekte (pasif dinleme özelliği) ve aynı zamanda veri paketlerini de toplayabilmektedir. Daha sonra bu paketler şifreleri çözülmek üzere başka programlarda kullanılabilmektedir. Şekil 5.1'de "Kismet" programının bir ekran görüntüsü verilmiştir.



Şekil 5.1. “Kismet” programı

5.1.1. WEP Anahtarının Elde Edilmesi

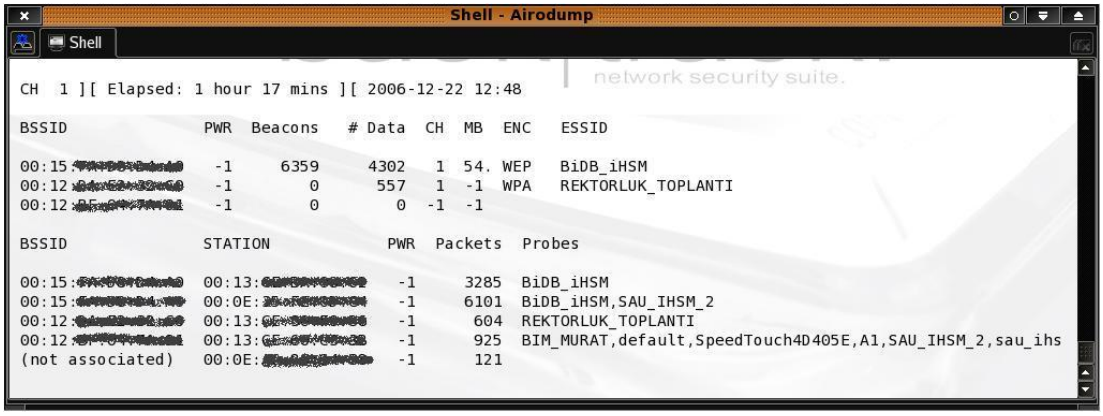
“Kismet” programı ile ağ ortamı hakkında bilgiler elde edildikten sonra, paket toplama işini daha iyi yapan “airodump” programı ile ağ trafiğinden paketler toplanmıştır. “airodump” programının kullanımı “airodump [options] <interface>” şeklindedir. [options] kısmı; toplanacak paketlerin kaydedilme özellikleri, kaydedilecek dosyanın adı, çalışılacak kanal numarası ve çalışma frekansı gibi

seçenekleri sunar. <interface> kısmı ise saldırı yapan ağ arabirim kartını belirtmek için kullanılır.

Bu çalışmada kullanılan komut:

airodump –ivs /ivpacket eth0;

şeklindedir. –ivs komutu, toplanan paketlerden sadece IV bilgilerinin alınmasını belirtmektedir. /ivpacket, toplanan paketlerin çalışılan klasörde ivpacket.ivs dosyasına kaydedileceğini belirtmektedir. WEP anahtarının elde edilmesi için IV'lerin bilinmesi yeterlidir. "airodump" programına ilişkin ekran görüntüsü Şekil 5.2'de verilmiştir.



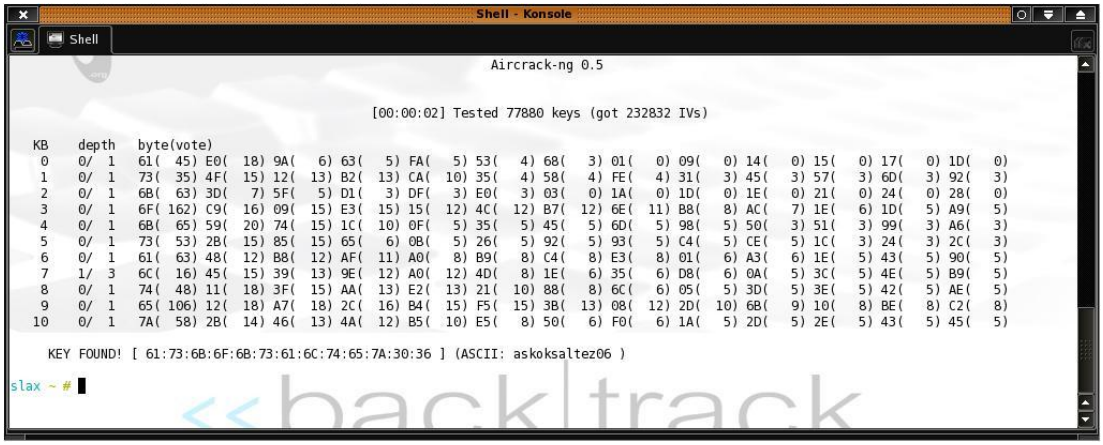
Şekil 5.2. "airodump" ekran görüntüsü

Yeterli paket toplandıktan sonra "aircrack" programı kullanılarak WEP anahtarı elde edilmeye çalışılmıştır. "aircrack" programının kullanımı "aircrack [options]" şeklindedir. [options] kısmı çözülecek şifreyle ilgili bilgileri ve kullanılacak dosyaları belirtir.

Bu çalışmada kullanılan komut:

aircrack –a 1 –n 64 /*.ivs

şeklindedir. –a parametresi şifreleme türünü belirtir; 1 değerini aldığında WEP, 2 değerini aldığında WPA şifreleme kullanıldığı anlamına gelir. –n parametresi, şifrelemenin kaç bit ile yapıldığını belirtir; 64/128 değerlerini alır. *.ivs parametresi, çalışılan klasördeki tüm "ivs" uzantılı dosyaların değerlendirileceği anlamına gelir. Bunun yerine, "cab" uzantılı dosyalar da kullanılabilir. Bu özellik sayesinde, farklı zamanlarda toplanan paketler de aynı oturumda kullanılabilmektedir. Okunan bu dosyalar içinde birden fazla kablosuz ağa ait paketler olabilir. "aircrack" programı, dosyaları okuduktan sonra, paketlerin toplanmış olduğu ağların bir listesini vererek; istenen ağa ait verilerin kullanılmasını ve dolayısıyla yine o ağa ait WEP anahtarının elde edilmesini sağlamaktadır. "aircrack" programının ekran görüntüsü Şekil 5.3'te verilmiştir. Yapılan çalışmalarda, 64 ve 128 bit WEP anahtarlarının elde edilmesi için sırasıyla, yaklaşık olarak 150.000 ve 230.000 IV paketi toplanması gerekmiştir.



Şekil 5.3. "aircrack" ile WEP anahtarının elde edilmesi

Bu tez çalışmasında kullanılan her iki ağ için, WEP anahtarı aynı yöntemle elde edilmiştir. Birinci ağ (Sakarya Üniversitesi bünyesindeki kurumsal ağ) için WEP anahtarı elde edildikten sonra, internet erişimi sağlanmıştır. Bu ağı kullanan gerek kurum çalışanları gerekse misafirlerin bilgisayarlarına bilinen yöntemlerle saldırıda bulunulabilir. Ancak kablolu ağa erişilmek istendiğinde, kullanılan güvenlik duvarı sayesinde bu istekler reddedilmektedir. Bununla birlikte hem kablolu ağa hem de kablosuz ağa bağlı ve hiçbir güvenlik önlemi almayan bir çalışanın bilgisayarı üzerinden kablolu ağa sızmak mümkündür. Kurbanın bilgisayarına yüklenecek bir trojan ile bu gerçeklenebilir. WEP anahtarı elde edildikten sonra yapılabilecek

saldırılar aynı zamanda kablolu ağlar için de geçerlidir ve bu tezin konusu gereği sadece kablosuz ağla ilgili saldırılar uygulanmıştır.

İkinci ağ (orta ölçekli şirket ağı örneği) için WEP anahtarı elde edildikten sonra internet erişimi sağlanmıştır. Bu ağda herhangi bir güvenlik duvarı olmadığı için yapılandırılacak kablolu ağa erişim de kolaylıkla sağlanabilmektedir.

Her iki ağda yapılan çalışmalarda, en büyük sorun ağ trafiği hakkında olmuştur. Özellikle ikinci ağdaki trafiğin gereken miktardaki paketleri kısa zamanda toplamak için yeterli yoğunlukta olmaması, farklı bir yöntem kullanmayı gerektirmiştir. Bu sorunu çözmek için "aireplay" adlı program kullanılmıştır. "aireplay" ile STA-AP arasında iletilen paketler yakalanıp, tekrar tekrar ve farklı istasyonlardan gönderiliyormuş gibi simüle edilerek yoğun bir ağ trafiği oluşturulmuştur.

Yapılan uygulamalarda, her iki ağ için farklı kombinasyonlarda yapılan yapılandırma Tablo 5.1'de verilmiştir.

Tablo 5.1. Deneylerde kullanılan ağların yapılandırmaları

SSID Yayını	**MAC Filtreleme**	**Anahtar Uzunluğu**	**Şifreleme**	**Sonuç**
Evet	Hayır	64 bit	WEP	Başarılı
Evet	Hayır	128 bit	WEP	Başarılı
Hayır	Evet	64 bit	WEP	Başarılı
Hayır	Evet	128 bit	WEP	Başarılı

SSID Yayını: SSID yayını yapılmayan durumlarda pasif dinleme yapan "Kismet" programı ile öncelikle SSID elde edilmiştir.

MAC Filtreleme: MAC adresi filtrelemesi yapılan durumlarda, yine "Kismet" programı ile ağ dinlenerek yetkili kullanıcılara ait MAC adresleri tespit edilmiştir. WEP anahtarı elde edildikten sonra, bu yetkili MAC adreslerinden biri, saldırı yapan

bilgisayara atanarak ağa erişim sağlanmıştır. MAC adresi hem Windows hem de Linux işletim sistemlerinde sırasıyla Registry ve komut satırından değiştirilebileceği gibi bu işi otomatik olarak yapan programlar da mevcuttur.

Anahtar uzunluğu: Anahtarlar, 64 ve 128 bit uzunlukta ayrı ayrı belirlenmiş; her iki durumda da başarıyla elde edilmişlerdir. 128 bit anahtar kullanıldığında yaklaşık 2 kat daha fazla paket toplanması gerekmiştir.

5.1.2. WPA Anahtarının Elde Edilmesi

WPA anahtarının elde edilmesinde, WEP anahtarında olduğu gibi öncelikle kablosuz ağın dinleme programıyla tespit edilmesi gerekmektedir. Özellikle SSID yayını yapmayan AP'ler ile oluşturulan ağlarda bu çok önemlidir. WPA anahtarının elde edilmesi için yapılan çalışmalarda ilk önce, kullanılan her iki kablosuz ağda WPA şifreleme etkinleştirilmiştir.

WPA ile şifrelenmiş bir kablosuz ağın, WPA anahtarını elde etmek için öncelikle kullanılacak anahtar sözlüklerinin temin edilmesi gereklidir. Bu sözlükler, metin dosyası halinde hazırlanmaktadır ve piyasada ücretsiz olarak sunulmaktadır. İstendiğinde bu dosyalar saldırgan tarafından da hazırlanabilir. WPA anahtarı elde etmeye başlamadan önce iki farklı sözlük dosyası temin edilmiştir.

Bir sonraki adım olarak; ağın dinlenmesi aşamasında STA ve AP arasında bir asıllama (authentication) işleminin yapılması beklenmektedir. Asıllama işlemi sırasında ağda iletilen ve "handshake" adı verilen EAPOL mesajlarının yakalanması gerekir. Yakalanan bu mesajlar ve sözlük dosyaları birlikte kullanılarak WPA anahtarı elde edilebilir. Esasında, bu aşamadan sonra anahtarı ele geçirmek sadece sözlük dosyasının içeriğine bağlıdır. Sözlük dosyası ne kadar geniş ise, anahtarın bulunması ihtimali o kadar yüksektir. Bu da, teorik olarak bütün WPA anahtarlarının elde edilebileceği anlamına gelir.

EAPOL mesajlarının yakalanması için, WEP ile şifrelenmiş paketlerin yakalanmasında da kullanılan “airodump” programından faydalanılmıştır. Ancak bu sefer komut dizisi:
airodump /eapolpacket eth0

şeklindedir. Bu komutun görevi; ağda iletilen veri paketlerinin, çalışılan klasör içinde eapolpacket.cap dosyasına yazılmasını sağlamaktır. Toplanan bu paketler içinde bir adet asıllama işlemi verisinin (handshake) olması yeterlidir. Eğer kablosuz ağda uzun süre bir asıllama işlemi gerçekleşmezse, yine daha önce kullanılan “aireplay” programı kullanılabilir. Bu program ile o an için asıllanmış olan bir kullanıcıya, bağlı olduğu AP taklit edilerek sahte mesajlar gönderilir. Bu sahte mesajlar doğal olarak yanlış anahtarla şifrelenmiş olacağından, kullanıcı AP’yi yeniden asıllama işlemine zorlayacaktır ve yeni bir asıllama işlemi yapılacaktır. Bu asıllama işlemi sırasında, WPA anahtarını elde etmek için kullanacak olduğumuz “handshake” paketini elde etmiş oluruz.

Ancak yapılan çalışmalarda görülmüştür ki; “airodump” her zaman EAPOL mesajlarını yakalayamamaktadır. Bu sorunun çözümü, “ethereal” programının kullanılmasıyla sağlanmıştır. Grafik arabirimli “ethereal” hem Linux hem de Windows’ta çalışabilmektedir ve WPA EAPOL paketlerini tam bir başarıyla yakalayıp kaydedebilmektedir. Şekil 5.4’te “ethereal” programı ile paketlerin yakalanması (capture işlemi) gösterilmiştir.

“airodump” ve/veya “etheral” programı ile istenen veri paketi elde edildikten sonraki aşama, bu paketi sözlük dosyaları ile harmanlayıp şifresini çözmektir. Bu işlem için iki farklı program kullanılmıştır. Birincisi, “aircrack”, ikincisi “cowpatty” programıdır. “aircrack” programı WEP anahtarı elde etmede de kullanılmıştı. Bu sefer programda kullanılan komut dizisi:

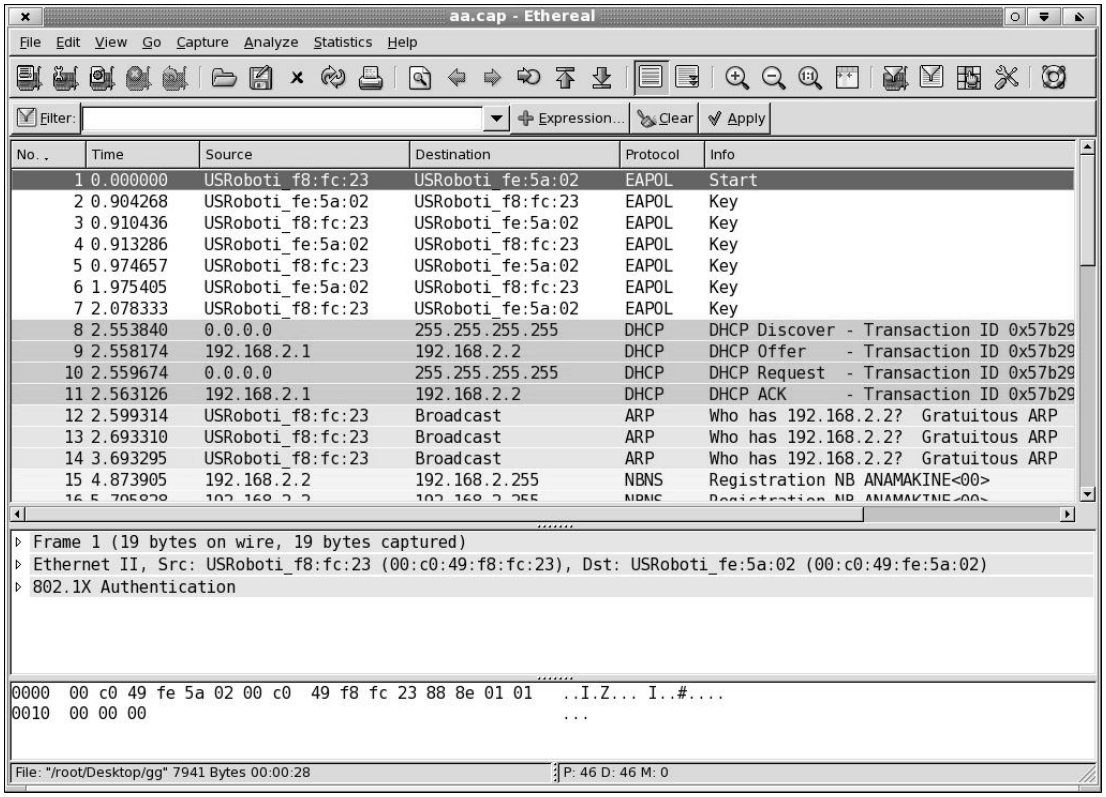
aircrack –a 2 –w /dictionary.txt /eapolpacket.cap

şeklindedir. –a 2 parametresi, şifreleme türünün WPA olduğunu belirtir. –w parametresi de sırasıyla kullanılacak sözlük dosyasını ve yakalanmış paket dosyasını tanımlar.

“cowpatty” programının komut dizisi:

cowpatty –f /dictionary.txt –r /eapolpacket.cap –s SSIDadı

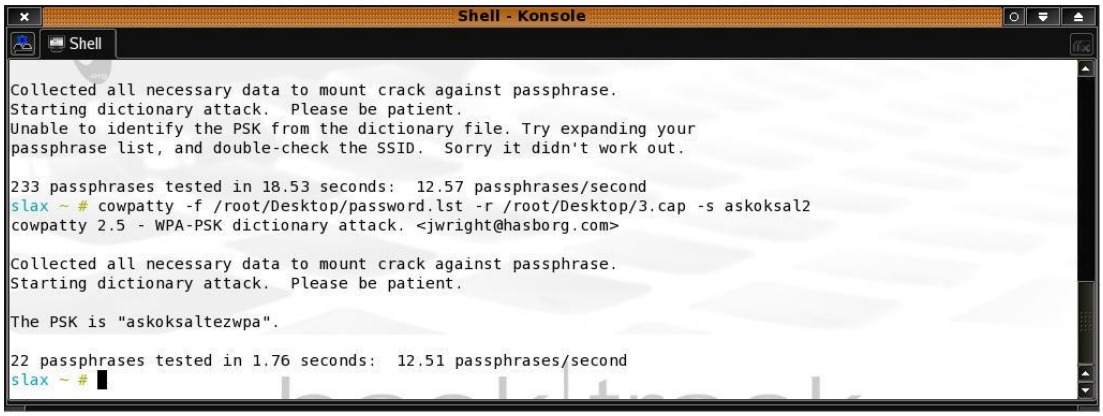
şeklindedir. –f parametresi ile kullanılacak sözlük dosyası; -r parametresi ile yakalanmış paket dosyası; -s parametresi ile de ağ adı belirtilmektedir.



Şekil 5.4. “ethereal” ile paketlerin yakalanması

Yapılan deneylerde, her iki program da kullanılmıştır. Farklı iki program kullanarak hem her iki programın performansları karşılaştırılmış hem de birbirlerine göre bazı farklılıklar tespit edilmiştir. Performans olarak her iki programın yaklaşık olarak aynı oldukları gözlenmiştir. Ancak “airodump” programı Windows ortamında toplanan

paketleri okuyamazken “cowpatty” programında bu uyumsuzluk yoktur. “cowpatty” programı ile şifresi çözülen bir WPA anahtarı Şekil 5.5’te gösterilmektedir.



Şekil 5.5. “cowpatty” ile WPA anahtarının elde edilişi

Deneyler sırasında farklı WPA anahtarları kullanılarak çok sayıda ağ yapılandırılması yapılmıştır. Bu deneylerden de anlaşılmıştır ki, EAPOL asıllama paketleri (EAPOL handshake) elde edildikten sonra, iş sadece sözlük dosyalarına kalmaktadır. Deneyler sırasında iki farklı sözlük dosyası kullanılmıştır. Bu dosyalardan birincisi küçük boyutlu, ikincisi ise oldukça büyük boyutludur. Dosya boyutu büyüdükçe görülmüştür ki, anahtarın elde edilmesi bu dosyanın boyutuna ve anahtarın dosyanın neresinde olduğuna bağlıdır. Çünkü sözlük dosyası, sıralı olarak anahtarla harmanlanmaktadır.

Yapılan deneylerin hepsinde WPA anahtarı elde edilememiştir. Bunun da nedeni sözlük dosyalarının yetersizliğidir. Esasında, saldırganın zaman sıkıntısı olmadıkça, milyonlarca kelimeden oluşturabileceği bir sözlük veritabanını kullanarak bütün WPA anahtarlarını elde edebilir. Bunun da tek şartı ağ trafiğinde bir EAPOL mesajı yakalamak olduğuna göre ve zaman da bol olduğuna göre WPA şifrelemenin WEP’ten çok güvenli olmadığı sonucuna varılabilir.

Ancak bu durum sadece WPA’nın ön paylaşımlı anahtar (pre-shared key – WPA-PSK) ile kullanılması durumunda geçerlidir. 4. bölümde de bahsedildiği üzere, WPA, gerek bir RADIUS sunucusu ile birlikte gerekse AES şifreleme ile birlikte kullanıldığında oldukça güvenli bir teknolojidir. WPA-RADIUS, WPA-AES, WPA2

(802.11i) güvenlik mekanizmalarına halen herhangi başarılı bir saldırı yapılamamış olması bunu kanıtlamaktadır.

5.2. Uygulama 2

Bu tez çalışması kapsamında gerçekleştirilen ikinci uygulamanın amacı, kullanımda olan kablosuz ağlar hakkında bilgiler toplamak ve bu bilgiler ışığında kablosuz ağ güvenliği konusunda bir sonuca varabilmektir. Uygulama, Sakarya il merkezinde belirlenen işlek caddelerde yapılmıştır.

Uygulama, söz konusu merkezlerde, Intel pro2200 802.11b/g wireless adapter'e sahip dizüstü bilgisayar, Linux işletim sistemi ve Kismet programı kullanılarak gerçekleştirilmiştir. Birinci uygulamada da kullanılan Kismet programı, bu uygulamada da kablosuz ağların hem aktif hem de pasif olarak dinlenmesi ve bu ağlara ait bazı verilerin toplanması amacıyla kullanılmıştır. Kismet programı ile kablosuz ağlar hakkında toplanan bu veriler aşağıda sıralanmıştır:

- Ağın tipi
- Ağın adı (SSID)
- AP'nin MAC adresi
- AP'nin IP adresi
- Yayın yapılan kanal
- Şifreleme türü
- Bağlantı hızı
- İletilen veri bilgileri
- Ağın çalışma zamanı, konumu, gürültü seviyesi vs.

Bu tezin kapsamı gereği yapılan çalışmada kablosuz ağların şifreleme türleri dikkate alınmıştır. Toplanan veriler analiz edilerek, mevcut kablosuz ağların hangi güvenlik önlemlerini aldıkları tespit edilmiştir. Tablo 5.2 incelenen ağlardaki güvenlik önlemleri hakkında bilgiler içermektedir.

Tablo 5. 2. İncelenen ağların analizi

	Şifreleme Türü				Toplam Ağ Sayısı
	Şifresiz	**WEP**	**WPA**	**WPA2**	
Adet	74	44	20	13	151
%	49	29,14	13,25	8,61	100

Yapılan uygulama sonucunda mevcut kablosuz ağların %49'unda şifreleme yapılmadığı (Açık Erişim) ancak bu ağların %28,3'ünün SSID yayını gizlenerek güvenliklerinin sağlanmasına çalışıldığı görülmüştür. Aynı şekilde WEP şifreleme kullanan ağların %5'inin de SSID yayını gizlenerek koruma altına alınmaya çalışıldığı gözlenmiştir. Halbuki SSID yayını gizlemenin çok zayıf bir güvenlik önlemi olduğu önceki bölümde gösterilmişti. Bu tablo, inceleme yapılan bölgedeki ağların %78,14'ünün güvenli olmayan Açık Erişim ve WEP şifrelemeyi tercih ettiğini göstermektedir. Bununla birlikte yine tam güvenlik sağlamayan WPA şifrelemenin de eklenmesiyle, bütün kablosuz ağların %91,39'unun güvenliği tam olarak sağlanmamış ağlar olduğu sonucuna varılabilir.

5.3. Güvenli Bir Kablosuz Ağ Yapılandırma Örneği

Bu tez çalışması kapsamında yapılan ikinci uygulama sonuçlarından, kablosuz ortamda tespit edilen ağların çok büyük bir kısmının ev, küçük ve orta ölçekli şirketlerde yapılandırıldığı anlaşılmıştır. Yine bu ikinci uygulama sonuçlarından, yapılandırılan kablosuz ağların büyük kısmının güvenli olmadığı tespit edilmiştir. Bu olumsuz durumun giderilebilmesi amacıyla, bu tez çalışmasında üçüncü olarak, günümüzde tam güvenlik sunan bir yapılandırmanın, bu kısımda detaylı olarak sunulması faydalı görülmüştür.

Yapılandırılan kablosuz ağda kullanılan Erişim Noktası (Access Point - AP) USRobotics Maxg Router – USR5461'dir. Güvenlik mekanizması olarak ise 802.11i (WPA2) seçilmiş ve bunun yanı sıra AP'nin sunmuş olduğu ek güvenlik seçenekleri de değerlendirilmiştir.

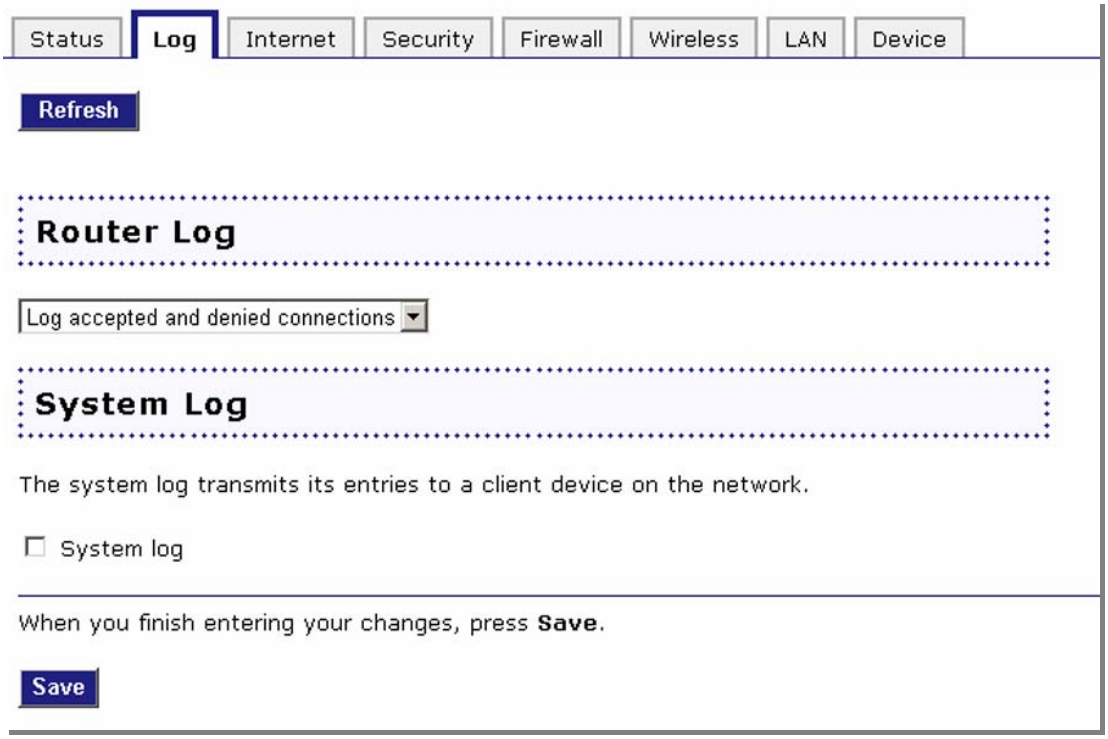
Kullanılan AP'ye erişim web ortamından yapılmaktadır, Erişim adresi http://192.168.2.1 herhangi bir web tarayıcı ile AP'nin bağlı olduğu bilgisayar üzerinden açılabilmektedir. Bu noktadan sonra kablosuz ağın yapılandırılması adım adım anlatılacaktır.

Log (Günlük) Ekranı:

Log, ağdaki çeşitli trafik şekillerinin takip edilmesi için kullanılan bir yöntemdir. Örneğin, yetkisi olmayan hangi kullanıcıların ağa erişmeye çalıştığını bilmek ya da yetkisi olan kullanıcıların ağa ne zaman eriştiklerini bilmek için bu özellik yararlı olabilir. Router Log alanında, No Log (Günlük Tutma), Log denied connections only (Sadece reddedilen bağlantıların günlüğünü tut), Log accepted connections only (Sadece kabul edilen bağlantıların günlüğünü tut) ya da Log accepted and denied connections (Kabul edilen ve reddedilen bağlantıların günlüğünü tut) seçenekleri vardır.

System Log alanındaki onay kutusu seçilirse bir IP adresi girilmesi gerekecektir. Bu seçenek, meydana gelen tüm sistem olaylarının günlüğünü tutar ve bu günlüğü belirtilen IP adresine gönderir.

Bizim yapılandırmamızda hem kabul edilen hem de kabul edilmeyen kullanıcıların izlenebilmesi açısından Router Log alanında "Log accepted and denied connections" seçeneği seçilmiştir.

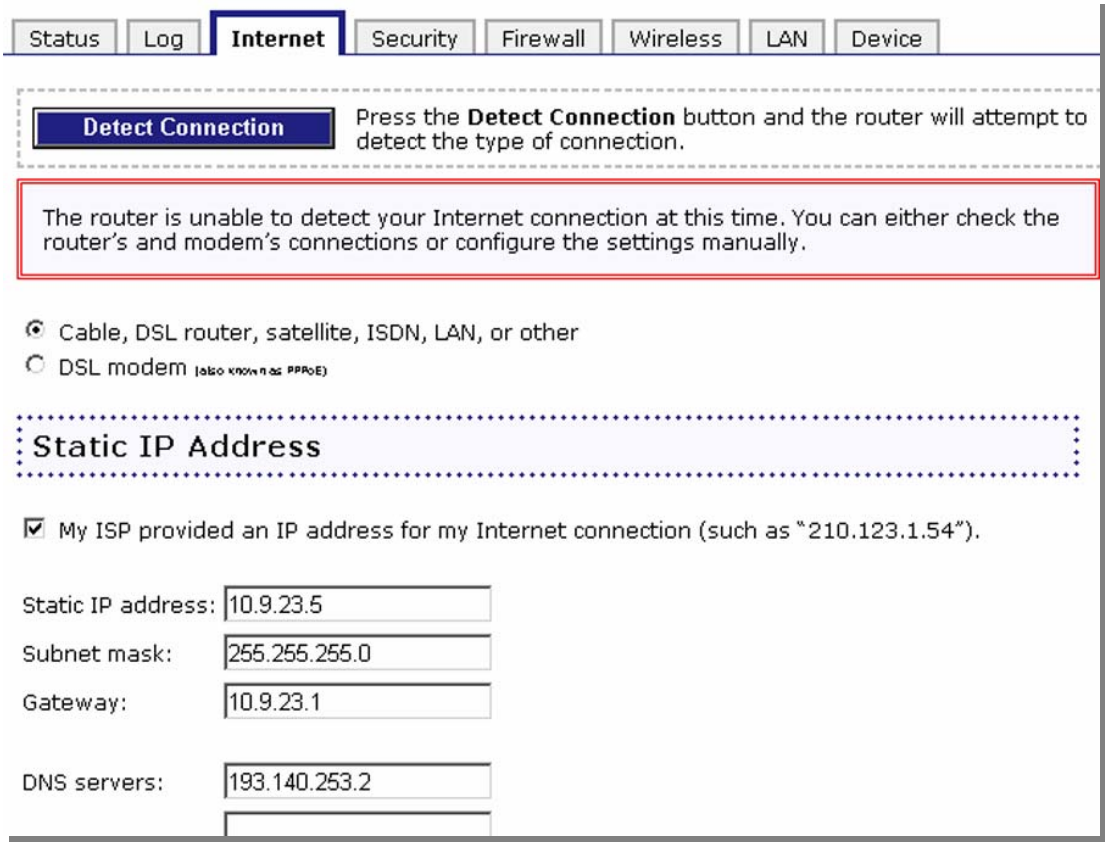


Şekil 5.6. Log ayarlarının yapılması

Internet Ekranı:

Bu ekranda öncelikle Detect Connection (Bağlantıyı Algıla) butonu ile otomatik olarak IP ayarları yapılandırılabilir. Bu işlem başarısız olursa sistem yöneticisi veya servis sağlayıcısı tarafından bildirilen IP ayarları "Static IP Address" alanına elle girilebilir.

Internet alanında ayrıca, servis sağlayıcı tarafından isteniyorsa, Ana Bilgisayar Adı "Host Name" kısmına, Kopya MAC Adresi "Clone MAC Address" kısmına, Kullanıcı Adı ve Şifre "Internet Login" kısmına girilmelidir. Bu alanda AP'ye uzaktan erişim için bulunan "Remote Access" kısmının kullanılması güvenlik açısından riskli olduğu için pasif tutulması önerilir.



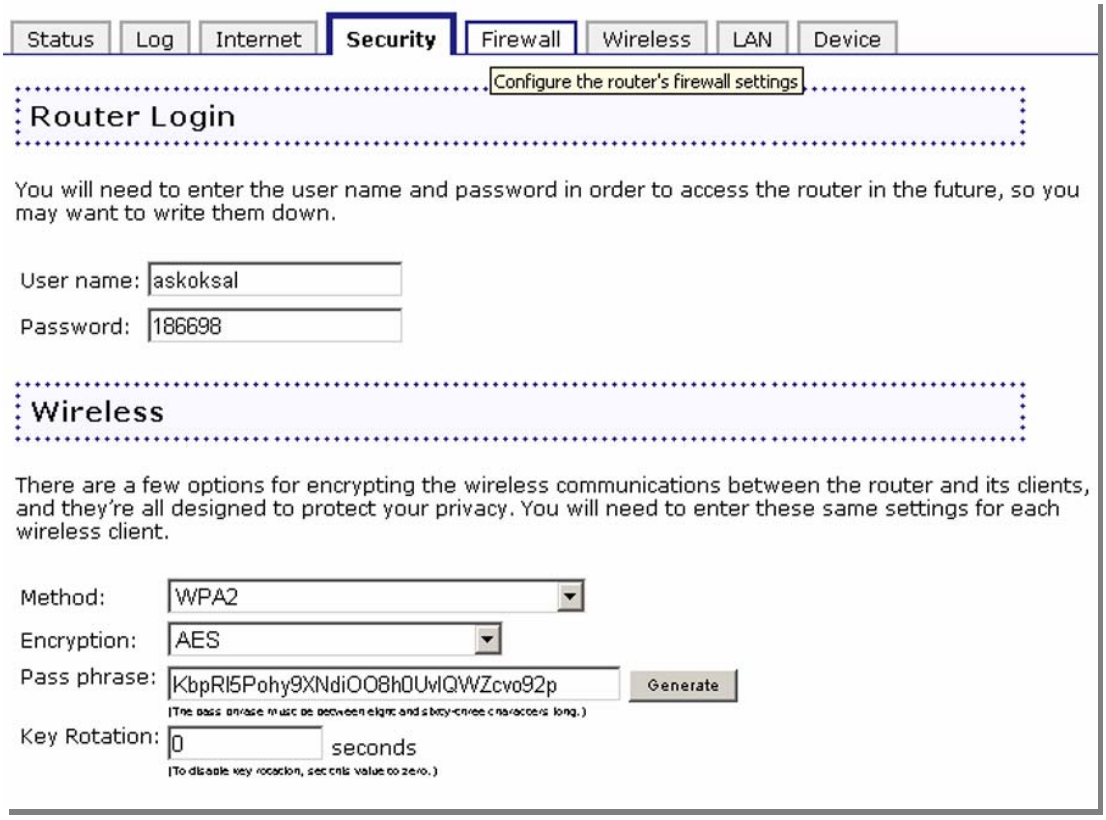
Şekil 5.7. İnternet bağlantı ayarlarının yapılması

Security (Güvenlik) Ekranı:

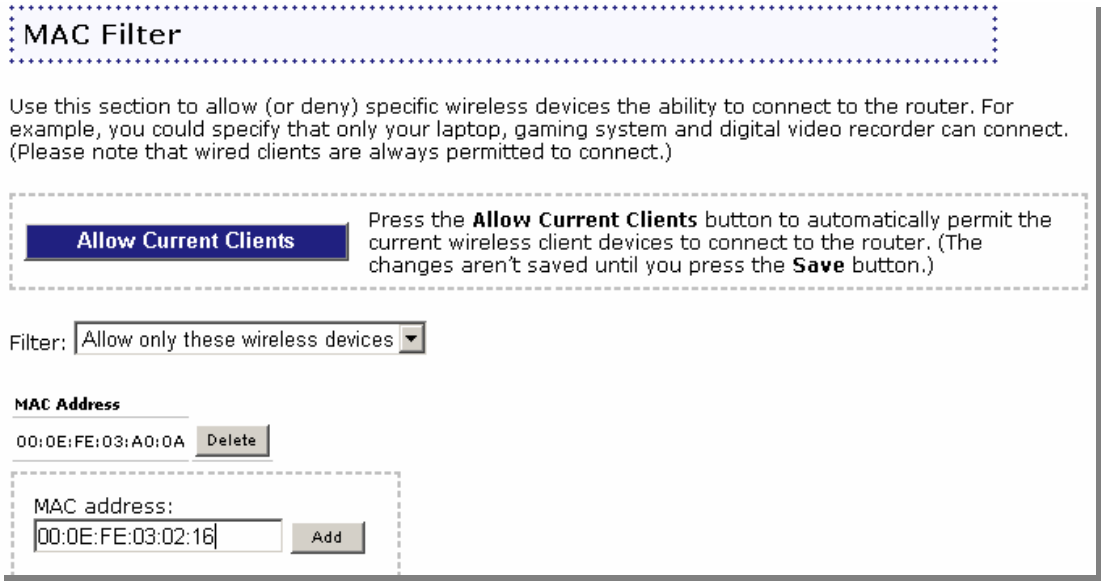
Bu bölümde ilk olarak, AP yönetim ekranına erişimde kullanılacak kullanıcı adı ve şifre, "Router Login" alanına girilmelidir. "Wireless" alanı AP'nin yapılandırılmasında dikkat edilecek en önemli güvenlik ayarlarını ihtiva eder. Bu uygulamada tercih edilen güvenlik mekanizması WPA2'dir. Bu sebeple yöntem olarak WPA2, şifreleme algoritması olarak da AES seçilmiş ve kablosuz iletişimde kullanılacak oturum anahtarı belirlenmiştir.

Security ekranında ek olarak MAC adreslerinin filtrelenmesi özelliği de kullanılabilir. "Wireless MAC Filter" kısmında bulunan "Filter", Allow all wireless devices (Tüm kablosuz aygıtlara izin ver), Allow only these wireless devices (Sadece bu kablosuz aygıtlara izin ver) ya da Deny only these wireless devices (Sadece bu kablosuz aygıtlara izin verme) seçenekleri ile istenilen yapılandırma yapılabilir. Bizim yapılandırmamızda "Allow only these wireless devices" seçeneği seçilerek

sadece izin verilen kullanıcıların kablosuz ağa erişebilmesi hedeflenmiştir. Daha sonra izin verilen MAC adresleri bu kısımda tanımlanmıştır.



Şekil 5.8. Güvenlik ayarlarının yapılması



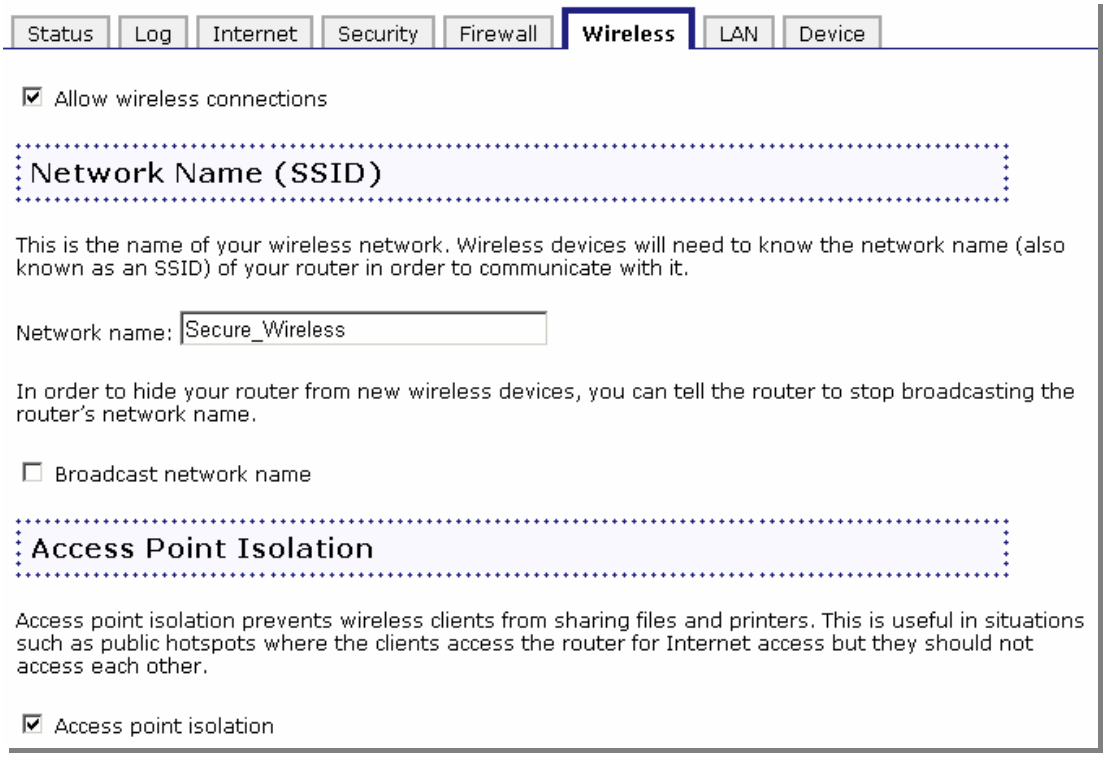
Şekil 5.9. MAC filtreleme işleminin yapılması

Wireless (Kablosuz) Ekranı:

Bu uygulamada kullanılan USR5461 model AP ayrıca 4-portlu kablolu bağlantıya izin verir. Bu ekrandaki "Allow wireless connections" (Kablosuz bağlantılara izin ver) seçeneği kaldırılırsa sadece kablolu bağlantı sağlanabilmektedir.

Güvenlik açısından bu ekranda yapılacak ayar Network Name (SSID) alanındaki "Broadcast network name" (Ağ ismini yayınla) seçeneği ile yapılmaktadır. Bu seçenek kaldırılarak ağ adının ortamda yayınlanması engellenmiştir. Bu şekilde yetkisiz kullanıcıların kablosuz ağımızı saldırı yöntemlerini kullanmadan görmesi engellenmektedir.

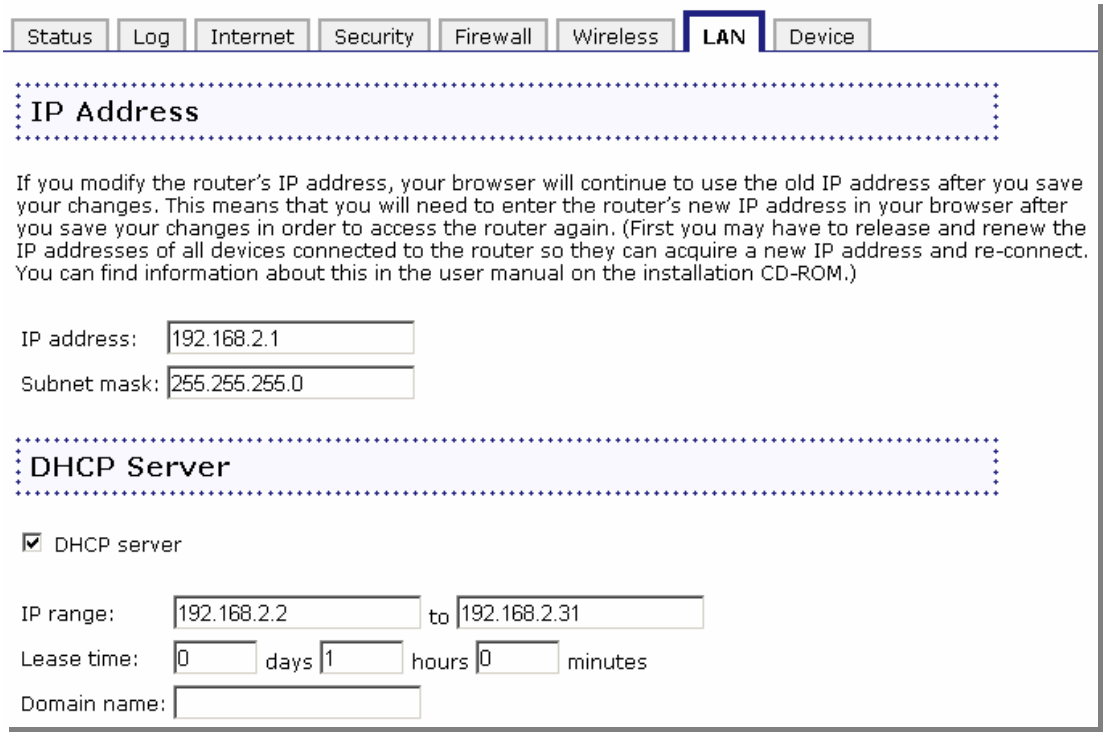
Bu ekrandaki diğer güvenlik önlemi "Access Point Isolation" (Erişim Noktası İzolasyonu) seçeneğinin seçilmesiyle alınmaktadır. Bu özellik ile, tüm kablosuz istemciler sadece internet erişimine sahip olacak, bu istemcilerin dosya ya da yazıcı paylaşımına erişim hakları olmayacaktır.



Şekil 5.10. Kablosuz ayarların yapılması

LAN Ekranı:

Bu ekranda kablolu bağlantıya ait ayarlar yapılmaktadır. IP adresi, alt ağ maskesi bilgilerinin yanı sıra kullanımına izin verilecek IP bloğu da bu alanda seçilebilmektedir.

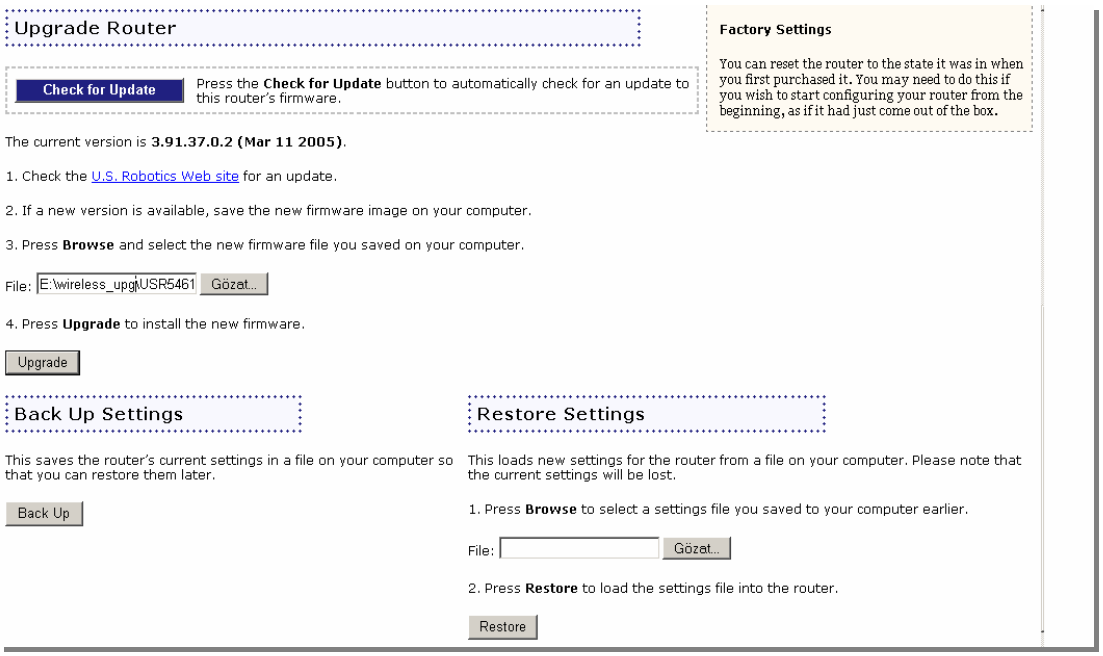


Şekil 5.11. LAN ayarlarının yapılması

Device (Aygıt) Ekranı:

Bu ekranda oldukça önemli olan fakat kullanıcıların genellikle ihmal ettikleri aygıt güncellemesi ayarı bulunmaktadır. Aygıt güncellemesi ile aygıtın üretiminden sonra, üretici tarafından yapılmış olan güvenlik ve diğer özelliklerdeki düzeltmeler elde edilmektedir. Birçok AP aygıtının özellikle güvenlik hususunda güncellemelerinin sürekli yapılıyor olması bu özelliği daha da önemli kılmaktadır. Bu özellik ile aygıta ait tespit edilen açıklar giderilebilmektedir.

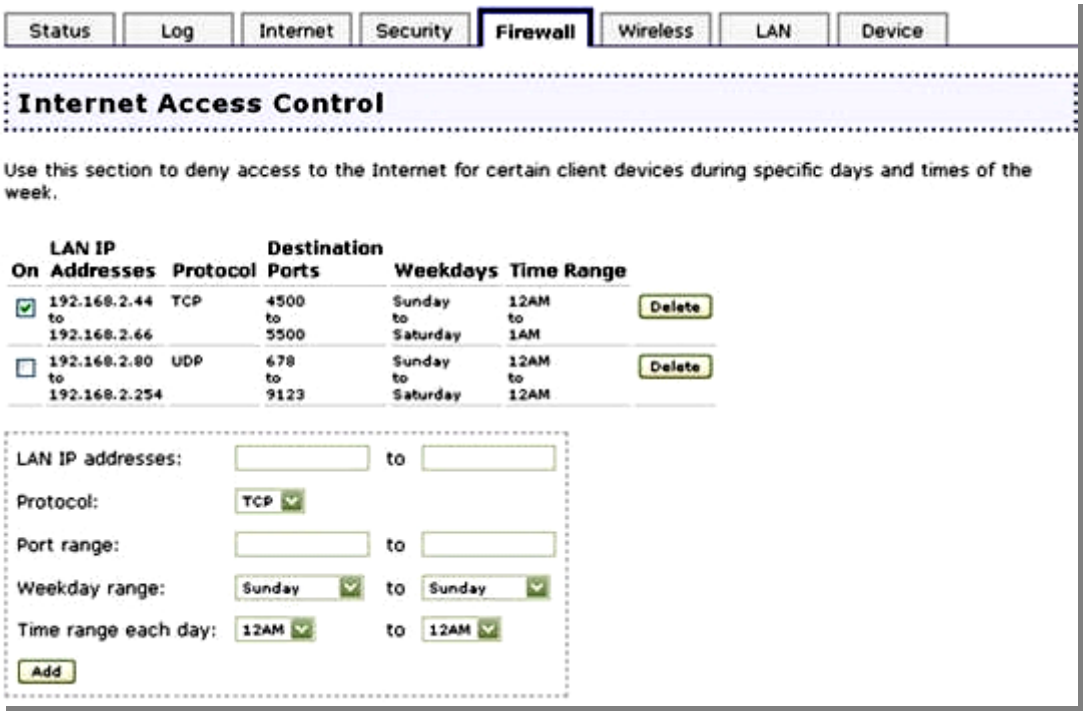
Bu alanda, internet üzerinden çevrimiçi olarak veya internet bağlantısı yoksa harici bir ortama kaydedilmiş güncelleme dosyasının belirtilmesiyle aygıt güncellemesi yapılabilmektedir.



Şekil 5.12. Aygıt güncellemesinin yapılması

Firewall (Güvenlik Duvarı) Ekranı:

Bu uygulamada kullanılan AP, kendine ait bir güvenlik duvarı uygulaması ile birlikte gelmektedir. Bu kısımda bulunan Internet Access Control alanında, haftanın belirli bazı günleri ve zamanlarında bazı istemcilere internet erişimi izinleri tanımlanabilmektedir.



Şekil 5.13. Güvenlik duvarı ayarlarının yapılması

BÖLÜM 6. SONUÇLAR VE ÖNERİLER

Kablosuz ağlar günümüzde olduğu gibi, sağladığı birçok avantajla birlikte gelecekte de vazgeçilmez iletişim teknolojisi olarak kalmaya devam edecektir. Bu yüzden kablosuz ağlar üzerinde sürekli araştırma – geliştirme çalışmaları yapılmaktadır. Yapılan çalışmalar ile en hızlı ve en güvenilir bir ağ iletişimi hedeflenmektedir.

Bu tez çalışması süresince 802.11 kablosuz ağlarında güvenlik konusu ele alınmış, geliştirilen güvenlik mekanizmaları incelenmiş, farklı güvenlik mekanizmaları üzerinde iki uygulama yapılmıştır. Yapılan uygulamalar sonucunda görülmüştür ki; WEP ve WPA-PSK şifreleme teknikleri kablosuz ağlarda güvenliği temin etmemektedir. Güvenli bir kablosuz ağ oluşturmak için 802.11i veya diğer adıyla WPA2 standardının kullanılması gerekmektedir. Bu standart ile daha güçlü bir şifreleme algoritması olan AES ve kullanıcı ile erişim noktası arasında karşılıklı bir kimlik doğrulaması gerektiren 802.1x asıllama (authentication) yöntemi kullanılmaktadır.

Güvenli bir ağ kurmadan önce, ağda tehlike oluşturabilecek kullanıcı kitlesini belirlemekte fayda vardır. Bu kullanıcılar:

- Meraklı bilgisayar kullanıcıları
- Bant genişliği hırsızları
- Bilgisayar korsanları

Meraklı bilgisayar kullanıcıları, genellikle kötü niyetli olmayan ama her zaman için bir tehlike unsuru oluşturan kesimdir. Bu kullanıcılar genellikle teorik bir bilgiye sahip olmayan, hazır programlar ile ağa saldırı yapan kesimi oluştururlar.

Bant genişliği hırsızları, açık erişimli veya eksik yapılandırılmış kablosuz ağları yetkisiz olarak kullanan zararsız kesimdir. Bu kesim, amacı kablosuz ağdan yararlanmak olduğu için ağa zarar vermez. Ancak ağı yavaşlatan unsur olarak dikkate alınmaktadırlar.

Bilgisayar korsanları, kötü niyetli olmasalar dahi ağa büyük zararlar verebilecek kesimdir. Özellikle veri gizliliğinin önemli olduğu kurumsal ağlar, bu tür saldırganlara karşı önlem almak zorundadırlar.

Bu tez süresince yapılan ikinci uygulama, kablosuz ağların bilinçsiz bir şekilde ve %91.39 gibi neredeyse tamamı denebilecek bir oranda güvensiz olarak yapılandırıldığını göstermektedir.

Kablosuz bir ağ yapılandırmasında uygulanabilecek güvenlik mekanizmaları aşağıdaki gibidir:

1. Açık erişim
2. 64-128 bit WEP şifreleme (ortak anahtarlı asıllama ile),
3. WPA şifreleme (802.1x asıllama ile),
4. WPA şifreleme (802.1x asıllama ve RADIUS sunucu ile),
5. WPA2 şifreleme (802.1x asıllama ile)
6. WPA2 şifreleme (802.1x asıllama ve RADIUS sunucu ile),
7. VPN ve WPA2 şifreleme (802.1x asıllama ve RADIUS sunucu ile).

Kişisel kullanımdan en karmaşık kurumsal kullanıma kadar bu mekanizmalar ile güvenlik çözümleri sunulmaktadır. 1,2,3 numaralı çözümler güvenli değildir. 4 numaralı çözüm günümüzde güvenlidir ancak gelecek için tam bir güvenlik vaat etmemektedir. 5,6,7 numaralı çözümler tam güvenlik sağlamaktadır.

Küçük ölçekli şirketler ve kişisel kullanım için 5; orta ölçekli şirketler, ticari kuruluşlar için 6; veri gizliliğinin çok önemli olduğu büyük kurumlar için 7 numaralı çözüm kullanılmalıdır.

KAYNAKLAR

[1] ÖZTÜRK, E., Wlan Kablosuz Yerel Alan Ağları (Wıreless Local Area Networks) Teknolojisinin İncelenmesi, Mevcut Düzenlemelerin Değerlendirilmesi Ve Ülkemize Yönelik Düzenleme Önerisi. Telekomünikasyon Kurumu, Ekim 2004.

[2] MANAS, O., Kablosuz Yerel Alan Ağları ve Kablosuz Uygulama Protokolü (Wireless LAN And WAP). Ağustos 2002.

[3] TANENBAUM, A., Computer Networks. 4th Ed., Prentice Hall, 2002.

[4] MINOLI, D., Telecommunications Technology Handbook. Second Edition, Artech House, Boston London, s.245-335, 2003.

[5] ÖZDEMİR, M., Wireless LAN Technology & Security Update. Cisco Systems Inc., April 2003.

[6] ÇÖLKESEN, R., ÖRENCİK, B., Bilgisayar Haberleşmesi ve Ağ Teknolojileri. Papatya Yayıncılık, İstanbul, Ekim 2000.

[7] BAYILMIŞ, C., Kablosuz Bilgisayar Ağlarının Performans Analizi. Yüksek Lisans Tezi, Sakarya Üniversitesi, Haziran 2003.

[8] 802.11n: Next-Generation Wireless LAN Technology. White Paper, Broadcom Corp, April 2006.

[9] KURAN, M. S., TUGCU, T., A Survey on Emerging Broadband Wireless Access Technologies. Boğaziçi University, İstanbul, December 2006.

[10] XIAO, Y., IEEE 802.11n: Enhancements for Higher Throughput in Wireless LANs. The University of Memphis, December 2005.

[11] Raylink ,Frequency Hopping Spread Spectrum vs Direct Sequence Spread Spectrum. http://www.raylink.com/whitepaper/fhss_dsss.pdf

[12] http://www.wireless.per.nl/reference/chaptr05/ofdm/ofdm.htm.

[13] http://www.yasinkaplan.com.

[14] YILDIRIM, K.E., Linux Altında Kablosuz Bağlantı. İstanbul Teknik Üniversitesi Bilişim Enstitüsü. http://atlas.cc.itu.edu.tr/~mscelebi/est566/Lecture6.htm.

[15] THOMAS, T.M., Network Security First-Step. Chapter 8, Cisco Pres, 2004, http://mithras.itworld.com/download/book_chapters_and_wps /cisco _press/networksecurity_firststep_ch8.pdf.

[16] YÜKSEL, E., SOYTÜRK, M., OVATMAN, T., ÖRENCİK, B., Telsiz Yerel Alan Ağlarında Güvenlik Sorunu. İTÜ & Deniz Harp Okulu Komutanlığı, İstanbul.

[17] BARNES, C., BAUTTS, T., LLOYD, D., OUELLET, E., POSLUNS, J., ZENDZİAN, D.M., O'FARRELL, N., Hack Proofing Your Wireless Network. Syngress Publishing Inc., 2002.

[18] OLEXA, R., Implementing 802.11, 802.16 and 802.20 Wireless Networks - Planning, Troubleshooting and Operations. Elsevier Inc., Oxford 2005.

[19] RITZ, J.A., Introduction to the 802.11 Wireless Network Standard. CyberScience Laboratory, Rome 2003.

[20] KARYGIANNIS, T., OWENS, L., Wireless Network Security 802.11, Bluetooth and Handheld Devices. NIST Special Publication, 2002.

[21] Five Steps to Securing Your Wireless LAN and Preventing Wireless Threats. White Paper, Cisco Systems Inc., 2006.

[22] BARRETT, J., Wireless LAN Security Policy Template - Certified Wireless Network Professional. Planet3 Wireless Inc., 2003.

[23] JOSEPH, D., Deploying Secure 802.11 Wireless Networks with Microsoft Windows. Microsoft Pres, 2004.

[24] HURLEY, C., How to Cheat at Securing a Wireless Network. Syngress Publishing, Inc., 2006.

[25] EDNEY, J., ARBAUGH, W.A., Real 802.11 Security: Wi-Fi Protected Access and 802.11i. Addison Wesley, July 2003.

[26] GAST, M., 802.11 Wireless Networks: The Definitive Guide. O'Reilly, April 2002.

[27] BRIERE, D., HURLEY, P., Wireless Network Hacks & Mods For Dummies. Wiley Publishing, Inc., 2005.

[28] CHANDRA, P., Bulletproof Wireless Security GSM, UMTS, 802.11 and Ad Hoc Security. Elsevier Inc., 2005.

[29] PEIKARI, C., FOGIE, S., Maximum Wireless Security. Sams Publishing, 2002.

[30] DASGUPTA, P., BOYD, T., Wireless Network Security. Arizona State University.

[31] DE RANGO, F., LENTINI, D. C., MARANO, S., Static and Dynamic 4-Way Handshake Solutions to Avoid Denial of Service Attack inWi-Fi Protected Access and IEEE 802.11i. University of Calabria, Cosenza, Italy, June 2006.

[32] HE, C., MITCHELL, J. C., 1 Message Attack on the 4-Way Handshake. Stanford University, May 2004.

[33] LEHEMBRE, G., Wi-Fi security – WEP, WPA and WPA2. www.hakin9.org, June 2005.

ÖZGEÇMİŞ

1976 yılında Ordu'da doğdu. İlk, orta ve lise öğrenimini Ordu'da tamamladı. 1994 yılında Karadeniz Teknik Üniversitesi Mühendislik Mimarlık Fakültesi Elektrik-Elektronik Mühendisliği bölümünde lisans eğitimine başladı. 1998 yılında mezun oldu. 2004 yılında Sakarya Üniversitesi Fen Bilimleri Enstitüsünde lisansüstü eğitimine başladı. Halen Sakarya Üniversitesi'nde idari personel olarak çalışıyor.