T.C

TRAKYA ÜNİVERSİTESİ

FEN BİLİMLERİ ENTSTİTÜSÜ

KABLOSUZ AĞ TEKNOLOJİLERİ VE ŞİFRELEME

Deniz Mertkan GEZGİN

Doktora Tezi

Bilgisayar Mühendisliği Anabilim Dalı

Danışman: Yrd. Doç. Dr. Ercan BULUŞ

EDİRNE–2011

Doktora Tezi
Trakya Üniversitesi Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Bölümü

ÖZET

Bu tezin amacı, günümüzde yaygın olarak kullanılan kablosuz ağ teknolojilerini, bunların yapısını, kablosuz ağlarda kullanılan güvenlik standartlarını, kullanılan şifreleme metotlarını ve kablosuz ağlara karşı yapılan güncel saldırı tekniklerinin araştırılmasıdır. Bu amaç doğrultusunda Kablosuz ağlara yönelik bir DoS(Denial Of Service) saldırısı gerçekleştiren bir uygulama geliştirilmiştir. Bu yazılımın etkinliği ve deney sonuçları alınmıştır.

Tezin giriş kısmı olan birinci bölümünde kablosuz ağlar, kablosuz ağ kullanım alanları, Kablosuz Yerel Alan Ağlarında kullanılan donanımlar, kablosuz ağ teknolojileri ve kablosuz standartlar açıklanmıştır. IEEE 802. 11 kablosuz ağ standardı üzerinde durulmuş ve sınıflandırılması yapılmıştır.

Tezin ikinci bölümünde Kablosuz Yerel Alan Ağlarında(Wireless Local Area Network) kullanılan güvenlik politikaları ve şifreleme algoritmaları incelenmiştir.

Tezin üçüncü bölümünde Kablosuz Yerel Alan Ağlarına yapılan saldırı tipleri incelenmiş ve türlerine göre sınıflandırılmıştır.

Son bölümde Kablosuz Ağlara yapılan DoS saldırılarından Tcp, Udp, Kimlik Onaylamama (Deauthencation) Mesajı Taşması ve Ping Taşması saldırıları üzerinde durulmuştur. Bu saldırıların algoritmaları çıkartılmıştır. Bu saldırıların teorik açıklamalarından yola çıkılarak uygulamaları yapılmış ve hazırlanmış olan yazılım programları, performans analizleri ve sonuçlar verilmiştir.

Anahtar Sözcükler: Kablosuz Ağ Teknolojileri, WEP(Wired Equelancy Privacy), WPA(Wi-fi Protected Access), Kablosuz Ağlara Saldırılar, Servis Reddi(DoS), 802. 11

Yıl: 2011
Sayfa: 151

Doctorate Thesis
Trakya University Graduate School of
Natural and Applied Sciences
Department of Computer Engineering

ABSTRACT

The aim of this thesis is to investigate the widely used wireless network technologies; their structures, the safety standards used in those networks, the encryption methods used in wireless networks, and the current attack techniques against those networks. To this end, a DoS attack application to wireless networks was prepared. Its effectiveness and experiment results were recorded.

In the first section of the thesis, wireless networks, uses of those networks, the hardware used in Wireless Local Area Networks, wireless network technologies, and wireless standards were explained. IEEE 802.11 wireless network standard was focused and its classification was formed.

In the second section of the thesis, the safety policies used in Wireless Local Area Networks were investigated, and their encryption algorithms were described.

In the third section, the attack types to Wireless Local Area Networks were analyzed and classified according to their characters.

In the last section, the Denial of Service attacks; Tcp, Udp, De-authentication, and Ping overflow attacks were focused. Their algorithms were analyzed. With the theoretical explanations of those attacks, their applications were prepared. The prepared software applications, their performance analyses, and the results were reported.

Key Words: Wireless Network Technologies, WEP(Wired Equelancy Privacy), WPA(Wi-fi Protected Access), Wireless Network Attacks, DoS (Denial Of Service), 802. 11

Year: 2011
Page: 151

TEŞEKKÜR

Bu önemli ve güncel konuda çalışmamı sağlayan, bana yol gösteren, destek ve yardımlarını benden esirgemeyen, konu hakkındaki bilgisinden yararlandığım ve çalışma hayatımda bana her konuda destek olan danışman hocam Sayın Yrd. Doç. Dr. Ercan BULUŞ'a teşekkür ederim.

Tez izleme komitesinde ve tez jürisinde yer alan sayın hocalarım Doç. Dr Mümin ŞAHİN'e, Yrd. Doç. Dr. Tarık YERLİKAYA' ya, doktora çalışmalarım süresince yardımlarını esirgemeyen ve destek olan Yrd. Doç. Dr. M.Tolga SAKALLI, Yrd. Doç. Dr Andaç ŞAHİN MESUT'a, Arş. Gör. Fatma BÜYÜKSARAÇOĞLU SAKALLI' ya, Yrd. Doç.Dr. Halil Nusret BULUŞ'a tez çalışmama yaptıkları olumlu eleştiriler ile katkıda bulundukları için teşekkürlerimi sunarım.

Tez çalışmam zamanında maddi ve manevi olarak da olsa desteğini esirgemeyen meslektaşım Öğr. Gör. Elçin DOKSATLI'ya, değişik fikirleri ile bana bakış açısı sağlayan öğrencim Mehmet BAYRAKLI'ya ve bu yolda beni yüreklendiren, desteğini esirgemeyen Ayda SAĞDAN'a teşekkürlerimi sunarım.

Tez çalışmam sırasında bana her zaman destek olan babam Yusuf GEZGİN ve ablam Pınar GEZGİN'e çok teşekkür ederim.

Kalbimde her zaman sevgisini taşıdığım rahmetli canım annem Emel GEZGİN'e yanımda olduğunu bildiğim ve azmimi sağladığı için minnettarım.

Eylül 2011 **Deniz Mertkan GEZGİN**

ÖZET ..... **İİİ**

ABSTRACT ..... **V**

TEŞEKKÜR ..... **Vİİ**

TABLOLAR LİSTESİ ..... **Xİ**

ŞEKİLLER LİSTESİ ..... **Xİİ**

KISALTMALAR LİSTESİ ..... **XV**

1. GİRİŞ **1**

1.1 KABLOSUZ AĞLAR 1
1.2 KABLOSUZ AĞLARIN KULLANIM ALANLARI 4
1.3 KABLOSUZ HABERLEŞME TEKNOLOJİLERİ VE TÜRLERİ 5
1.3.1 IEEE (Institute Of Electrical And Electronical Engineers) Standartları 6
1.3.2 Kablosuz Kişisel Alan Ağları (WPAN-Wireless Personel Area Network) 8
1.3.2.1 IEEE 802.15 Standardı 8
1.3.2.2 Bluetooth (IEEE 802.15.1) 9
1.3.2.3 HomeRF 12
1.3.2.4 IrDA (Infrared Data Association) 13
1.3.2.5 ZigBee (IEEE 802.15.4) 15
1.3.2.6 Uwb (Ultra Wideband–802.15.3a) 16
1.3.3 Kablosuz Yerel Alan Ağları (WLAN-Wireless Local Area Network) 18
1.3.3.1 IEEE 802. 11 Standardı 19
1.3.3.2 HiperLAN 19
1.3.4 Kablosuz Anakent Alanı Ağları (WMAN- Wireless Metropolitan Area Network) 21
1.3.4.1 IEEE 802.16 Standardı 21
1.3.4.2 WiMAX (World Wide Interoperability for Microwave Access) 22
1.3.5 Kablosuz Geniş Alan Ağları (WWAN-Wireless Wide Area Networks) 24
1.3.5.1 IEEE 802.20 Standardı 24
1.3.5.2 GSM (Global System For Mobile Communication) 25
1.3.5.3 3G 25
1.3.5.4 GPRS (General Packet Radio Service) 26
1.4 IEEE 802.11 KABLOSUZ YEREL ALAN AĞ STANDARTLARI 27
1.4.1 IEEE 802.11 legacy 28
1.4.2 IEEE 802.11a 28
1.4.3 IEEE 802.11b 29
1.4.4 IEEE 802.11c 30
1.4.5 IEEE 802.11e 30
1.4.6 IEEE 802.11f 31
1.4.7 IEEE 802.11g 31
1.4.8 IEEE 802.11i 32
1.4.9 IEEE 802.11n 32
1.4.10 IEEE 802.11y 33
1.5 KABLOSUZ AĞLARDA MODÜLASYON TEKNİKLERİ VE YAPILARI 33
1.5.1 Doğrudan Sıralı Yayılı Spektrumu (DSSS-Direct Sequence Spread Spectrum) 34
1.5.2 Frekans Atlamalı Geniş Spektrum (FHSS-Frequency Hopping Spread Spectrum) 34
1.5.3 Dikey Frekans Bölüşümlü Çoğullama (OFDM-Orthogonal Frequency Division multiplexing) 35
1.5.4 Taşıyıcı Algılaması Çoklu Erişim/Çakışma Kaçınma (Csma/Ca-Carrier Sense Multiple Access/Collision Avoidance) 36

1.5.5 Çoklu Giriş Çoklu Çıkış (MIMO-Multiple Input Multiple Output) *36*
1.5.5.1 MIMO Temelleri 37
1.5.5.2 Maximum Ratio Combining (MRC) 37
1.5.5.3 Sinyal Oluşturma (Beamforming) 38
1.6 KABLOSUZ YEREL ALAN AĞLARDA ÇALIŞMA MODLARI VE AĞLAR 41
1.6.1 Tasarsız Mod (Ad Hoc Mode) *42*
1.6.1.1 Mobil Tasarsız Modlu Kablosuz Ağları 42
1.6.1.2 Kablosuz Duyarga Ağları (WSN-Wireless Sensor Networks) 43
1.6.1.3 Kablosuz Örgü Ağları (Wireless Mesh Networks) 43
1.6.2 Tasarlı Mod (Infrastructure Mode) *43*
1.7 KABLOSUZ YEREL ALAN AĞ TOPOLOJİLERİ 44
1.7.1 Yıldız Topolojisi (Star Topology) *44*
1.7.2 Örgü Topolojisi (Mesh Topology) *45*
1.8 KABLOSUZ ORTAM AĞ BİLEŞENLERİ 45
1.8.1 Kablosuz İstemci (Wireless Client) *46*
1.8.2 Kablosuz Erişim Noktası (WAP - Wireless Access Point) *46*
1.8.3 Kablosuz Tekrarlayıcı (Wireless Repeater) *48*
1.8.4 Kablosuz Köprüler (Wireless Bridges) *49*
1.8.4.1 Noktadan Noktaya (Point to Point) 49
1.8.4.2 Noktadan Çok Noktaya (Point to Multi Point) 50
1.8.5 Kimlik Doğrulama/Yetkilendirme Sunucusu (Authencation Server) *51*

2. KABLOSUZ AĞLARDA GÜVENLİK POLİTİKALARI VE ŞİFRELEME 52

2.1 SSID (SERVİCE SET IDENTİFİERS) GİZLEME 52
2.2 KABLOSUZ ERİŞİM NOKTASININ VARSAYILAN ŞİFRESİNİ DEĞİŞTİRMEK 54
2.3 MAC ADRES FİLTRELEME (MAC FİLTERİNG) 55
2.4 WEP (WİRELESS EQUEVİLEANT PRİVACY) ŞİFRELEMESİ 57
2.4.1 WEP'te Kimlik Doğrulama *57*
2.4.2 WEP'in Elemanları *59*
2.4.3 WEP'te Kullanılan Anahtarlar *60*
2.4.4 WEP'te Veri İşleme *61*
2.4.5 WEP'in Zayıflıkları *65*
2.4.6 RC4 Şifreleme Algoritması *66*
2.5 WPA (Wi-Fi PROTECTED ACCESS) ŞİFRELEMESİ 67
2.5.1 TKIP (Temporal Key Integrity Protocol) *70*
2.5.1.1 TKIP' de Veri İşleme ve Çalışma Prensibi 72
2.5.1.2 TKIP' de Anahtar Karıştırma İşlemi 73
2.5.1.3 TKIP' de Veri İletimi 75
2.5.1.4 Mesaj Bütünlük Kontrolü (MIC) 76
2.5.2 WPA'da Kimlik Doğrulama *77*
2.5.3 WPA'da Anahtar Yönetimi *81*
2.6 WPA2 (Wi-Fi PROTECTED ACCESS 2) ŞİFRELEMESİ (IEEE 802.11i) 84
2.6.1 CCMP (Counter Mode –Cbc Mac Protocol) *86*
2.6.2 AES (Advanced Encryption Standard) Şifreleme Algoritması *88*
2.7 WEP, WPA VE WPA2 KARŞILAŞTIRMASI 90

3. KABLOSUZ AĞLARA YAPILAN SALDIRI TÜRLERİ 91

3.1 KABLOSUZ AĞLARA YAPILAN SALDIRILARIN YÖNTEM VE TÜRÜNE GÖRE SINIFLANDIRILMASI 91
3.1.1 Erişim Kontrolü Saldırıları (Access Control Attacks) *92*
3.1.1.1 Kablosuz Ağları Tarama (War Driving) 93
3.1.1.2 Yetkisiz Erişim Noktası (Rogue Access Point) 93
3.1.1.3 Mac Adres Sahteciliği (Mac Spoofing) 94

3.1.1.4. Ip Adresi Yanıltma (Ip Spoofing) ... 95
3.1.1.5 Güvenli Olmayan Ağa Bağlanma (Adhoc Associations) ... 95
3.1.1.6 802.1x Radius Cracking ... 95
3.1.2 Gizlilik Saldırıları (Confidentiality Attacks) ... *96*
3.1.2.1 Gizli Dinleme (Eavesdropping) ... 96
3.1.2.2 Wep Anahtarı Kırma (Wep Key Cracking) ... 97
3.1.2.3 Şeytan İkizi Erişim Noktası (Evil Twin Ap) ... 97
3.1.2.4 Ap Üzerinde Sahte Portal Çalıştırmak (Ap Phishing) ... 97
3.1.2.5 Ortadaki Adam Saldırısı (Man In The Middle) ... 98
3.1.3 Bütünlük Doğrulama Saldırıları (Integrity Attacks) ... *98*
3.1.3.1 802.11 Paketi Püskürtme (Frame Injection) ... 98
3.1.3.2 802.11 Veri Tekrarlama (802.11 Data Replay) ... 99
3.1.3.3 802.1x EAP Tekrarlama (802.1x EAP Replay) ... 100
3.1.3.4 802.1x Radius Tekrarlama (802.1x Radius Replay) ... 100
3.1.4 Kimlik Doğrulama Atakları (Authentication Attacks) ... *100*
3.1.5 Kullanılabilirlik Saldırıları (Availability Attacks) ... *101*
3.1.6 Servis Reddi Saldırıları (DoS Attacks) ... *102*
3.1.6.1 DoS Atak Türleri ... 103
3.1.7 Dağıtık Servis Reddi Saldırıları (Distributed DoS Attack) ... *107*

4. KABLOSUZ AĞLARA YAPILAN SALDIRI (ATAK) UYGULAMALARI ... 108

4.1 WEP ŞİFRELEMESİNİN AİRCRACK PROGRAMI İLE KIRILMASI ... 108
4.2 WPA-PSK ŞİFRELEMESİNİN AİRCRACK PROGRAMI İLE KIRILMASI ... 110
4.3 OLUŞTURULAN BİR KABLOSUZ AĞ ORTAMI İLE GERÇEKLEŞTİRİLEN DOS ATAK UYGULAMALARI ... 114
4.3.1 Test Ortamı ... *114*
4.3.2 Kullanılan Saldırı Teknikleri ... *115*
4.3.2.1 Tcp Veri Tekrarı Taşması Saldırısı (Tcp Data Replay Flood Attack) ... 116
4.3.2.2 Ping Taşması Saldırısı (Ping Flood Attack) ... 118
4.3.2.3 Udp Taşması Saldırısı (Udp Flood Attack) ... 120
4.3.3 Dwl–2100 AP Cihazına Yapılan Saldırı Örneği ... *121*
4.3.4 DoS Saldırısı Deney Sonuçları ... *122*

5.SONUÇLAR ... 123

KAYNAKLAR ... 125

TEZ SIRASINDA YAPILAN ÇALIŞMALAR ... 133

ULUSLARARASI KONGRE VE SEMPOZYUM BİLDİRİLERİ ... 133
ULUSAL KONGRE VE SEMPOZYUM BİLDİRİLERİ ... 133

ÖZGEÇMİŞ ... 134

TABLOLAR LİSTESİ

Tablo 1. 1. IEEE 802 Kablosuz Ağlar Çalışma Grupları……..…7
Tablo 1. 2. IEEE 802. 15 Standartları……...8
Tablo 1. 3. ZigBee ile Diğer Kablosuz Teknolojilerin Karşılaştırılması……..…16
Tablo 1. 4.HiperLAN2 ile 802.11a standartlarının Karşılaştırılması……..20
Tablo 1. 5. WiMAX Standart Özellikleri…… ……..….23
Tablo 1. 6. WiMAX Erişim Özelliklerinin Karşılaştırılması…….…23
Tablo 1. 7. 802. 11 Kablosuz LAN Standartlarının Karşılaştırılması…….33
Tablo 2. 1. WEP, WPA ve RSN Karşılaştırması…….90
Tablo 3. 1. Erişim kontrolü saldırı çeşitleri…….92
Tablo 3. 2. Gizlilik Saldırıları (Confidentiality Attacks)……96
Tablo 3. 3. Bütünlük Doğrulama Saldırıları (Integrity Attacks)……..…..99
Tablo 3. 4. Kimlik Doğrulama Atakları (Authentication Attacks)……....101
Tablo 3. 5. Kullanılabilirlik Saldırıları (Availability Attacks)……..102
Tablo 4. 1 Saldırı için Açık olan bazı portlar ……...116

ŞEKİLLER LİSTESİ

Şekil 1. 1. Kablosuz Ağ Kategorileri ……6
Şekil 1. 2. Bluetooth Piconet Yapısı…… 11
Şekil 1. 3. Bluetooth Scatternet Yapısı…… 12
Şekil 1. 4. Kuzey Amerika UWB Spektrumu…… 18
Şekil 1. 5. MIMO'da Alıcı – Verici Yapısı…… 37
Şekil 1. 6. MRC Yapısı…… 38
Şekil 1. 7. İletken Sinyal Oluşturma…… 38
Şekil 1. 8. Yapıcı Karışma……..39
Şekil 1. 9. Yıkıcı Karışma…….. 39
Şekil 1. 10. Çoklu Yol…… 40
Şekil 1. 11. Çok-yollu Yayılım…….. 40
Şekil 1. 12. Uzaysal Çoklama…… 41
Şekil 1. 13. Tasarsız (Ad Hoc) Mod Yapısı…… 42
Şekil 1. 14. Tasarlı(Infrastructure) Mod Yapısı…… 44
Şekil 1. 15. Örgü (Mesh) Topolojisi…….. 46
Şekil 1. 16. Kablosuz Erişim Noktası…… 47
Şekil 1.17. Kablosuz Erişim Noktası Kullanım Modları…… 48
Şekil 1.18. Tekrarlayıcı Kullanılmış Kablosuz Ağ Örneği…… 49
Şekil 1.19. PtP Topolojisi İle Köprü Uygulaması…….. 50
Şekil 1.20. PtMP Topolojisi İle Köprü Uygulaması…… 51
Şekil 2.1. Gizlenmemiş SSID'li Kablosuz Erişim Noktası Yayını …… 52
Şekil 2.2. SSID Gizleme İşlemi……..53
Şekil 2.3. WEB Arayüzü İle Erişim Noktasına Giriş İşlemi…… 54
Şekil 2.4. Kablosuz Erişim Noktasının Default Şifresini Değiştirme İşlemi…… 54
Şekil 2.5. MAC Adresi İle Kimlik Doğrulama……..…… 55
Şekil 2.6. MAC Adres Filtreleme İşlemi……..…… 56
Şekil 2. 7. 802. 11 Açık Anahtar kimlik Doğrulaması…… 57
Şekil 2. 8. Ortak Anahtar Kimlik Doğrulaması…… 58
Şekil 2. 9. WEP Kullanarak Şifreleme İşlemi……. 59
Şekil 2.10 WEP'te Kullanılan Anahtar Çeşitleri……. 60

Şekil 2.11. WEP İşleyişi…… 61
Şekil 2.12. WEP MPDU Paketi Formatı…… 63
Şekil 2.13. WEP Şifrelemesi Blok Diyagramı…… 63
Şekil 2.14. WEP Şifre Çözümlemesi Blok Diyagramı…… 64
Şekil 2.15. Akış Şifreleme İşlemi…… 64
Şekil 2. 16. RC4 Algoritması Akış Şeması…… 68
Şekil 2. 19. TKIP Veri Şifreleme İşlemi…… 73
Şekil 2. 20. TKIP Anahtar Karıştırma İşlemi…… 74
Şekil 2. 21. TKIP Kapsüllenmiş Frame Yapısı…… 75
Şekil 2.22. Michael Algoritması…… 76
Şekil 2. 23. WPA-PSK Şifrelemesi AP Konfigurasyonu…… 77
Şekil 2.24. IEEE 802.1X İle Asıllama İşlemi…… 79
Şekil 2. 25. 802.1X Yapısı…… 80
Şekil 2. 26. 802.1X Denetimli /Denetimsiz Port…… 82
Şekil 2.27. 802.1X Anahtar Yönetimi Ve Dağıtımı…… 82
Şekil 2.28. Ana Oturum Anahtarı Düzeni…… 84
Şekil 2.29. AES Counter (sayaç) Çalışma Modu…… 86
Şekil 2.30. CCMP Çalışma Yapısı…… 87
Şekil 2.31. Tüm AES Algoritması (128 bit anahtar için)…… 89
Şekil 3. 1. TCP 3 Aşamalı Tokalaşma……104
Şekil 3. 2. TCP SYN Saldırısı……105
Şekil 4. 1. Airodump Programı Paket Toplama Ekranı……109
Şekil 4. 2. Aircrack Programı Şifre Bulunma Ekranı……110
Şekil 4. 3. Airodump Monitör modu Çalışma Komutu……111
Şekil 4. 4. Airodump Komutu İle Belirlenen AP'den Paket Toplama……112
Şekil 4. 5. Paket Toplama Ekranı (AP Listesi)……112
Şekil 4. 6. Aireplay Komutu İle Deauth Atak Komutu……112
Şekil 4. 7. Aircrack İle Toplanan Paketlerden Şifre Elde etme……113
Şekil 4. 8. WPA-PSK Şifresinin Bulunma Ekranı……113
Şekil 4. 9. Test Ortamı……114
Şekil 4. 10. Programın Akış Diyagramı……115
Şekil 4. 11. AP Bulma Ve Açık Port Arama Pseudo Kodları……116

Şekil 4. 12. Mac Adresi Bulma Fonksiyonun Pseudo Kodları.....117
Şekil 4. 13. Atağı Başlatma Pseudo Kodu.....117
Şekil 4. 14. Saldırı Sonuç Örneği Ekranı.....118
Şekil 4.15. Programın Access Point'te Ping Saldırısını Başlatması İçin Gerekli Kod.118
Şekil 4.16. Udp Taşma Saldırı Ekranı.....119
Şekil 4.17. Udp Flood Saldırısını Başlatmak İçin Gerekli Kod.....119
Şekil 4.18. TCP ve Ping Taşması Saldırısı Program Ekranı.....120
Şekil 4.19. Ping ve Udp Taşması Saldırısı Program Ekranı.....121
Şekil 4.20. Netmaster Kablosuz Modem Cihazına Yapılan Saldırı Sonuçları.....122
Şekil 4.21. Dwl–2100 AP Cihazına yapılan Saldırı Sonuçları.....122

KISALTMALAR LİSTESİ

AES	Advanced Encryption Standard
ANSI	American National Standards Institute
AP	Access Point
BSS	Basic Service Set
BSSID	Basic service set Identifier
CCMP	Counter mode and cipher-block chaining with message authentication code protocol
CRC	Cyclic redundancy check.
CSMA/CA	Carrier sense multiple access with collision avoidance
DHCP	Dynamic Host Control Protocol
DNS	Domain Name System
DSSS	Direct Sequence Spread Spectrum
DoS	Denial of Service
DDoS	Distributed Denial of Service
EAP	Extensible authentication protocol
ESS	Extented Service Set
ETSI	Europan Telecominications Standarts Institute
FHSS	Frequency-Hopping Spread Spectrum
GHz	Giga Hertz
GMK	Group master key
GSM	Global System for Mobile Communications
ICMP	Internet control message protocol
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISM	The industrial, scientific and medical
IV	Initialisation Vector
LAN	Local Area Network
LEAP	Lightweight EAP
MAC	Medium access control
MIMO	Multiple Input Multiple Output
OFDM	Orthogonal Frequency Division Multiplexing

PEAP	Protected EAP
PING	Packet internet groper
PSK	Pre-shared key
PTK	Pair wise temporal key
RADIUS	Remote authentication dial in user service
RSN	Robust security network
PC	Personal Computer
RF	Radio Frequency
SNMP	Simple network management protocol
SSID	Service Set Identifier
STA	Mobile Station
TCP	Transmission control protocol
TKIP	Temporal key integrity protocol
UDP	User datagram protocol
WEP	Wireless Equivalent Privacy
VLAN	Virtual Local Area Network
Wi-Fi	Wireless Fidelity
WiMax	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WPA	Wi-fi Protected Access
WPAN	Wireless Personel Area Network
WSN	Wireless Sensor Network
WWAN	Wireless Wide Area Network

1. GİRİŞ

Geçmişten günümüze bilgisayar ve buna bağlı olarak bilgisayar ağ teknolojilerinin popüler olduğu bir dönem mevcuttur. Geçmişe bakıldığında bilgisayar teknolojisindeki gelişmeler ENIAC, mainframe, PC (Personel Computer)'lere kadar dayanır. Günümüzde ise artık el bilgisayarı, netbook, PDA, Tablet PC ve işletim sistemi, hafızası bulunan cep telefonlarına kadar ilerlemiştir. Bu ilerlemeler ışığında bilginin paylaşımı gerekliliği ortaya çıkmış ve bilgisayar ağları konusu gündeme gelmiştir. Bunun paralelinde kablolu ağ iletişimi 2000'li yılların başına kadar çok popüler olup, günümüzde de yüksek hızlarda iletişim ofislere kadar inmiştir. Fakat kablolu iletişimin gerek alt yapı gerekse maliyeti, serbest dolaşımdan mahrum oluşu sayesinde bazı alanlarda kablosuz ağ teknolojileri gelişmiştir. İlk çıktığı, yaygın olmadığı zamanlarda düşük iletişim hızlarında bulunan kablosuz ağlar fazla pazar bulamamıştır. Fakat gün geçtikçe, gelişmelerle birlikte kullanım alanları ve iletişim hızları artmış, kablolu ağlara alternatif olmaktan çok bazı durumlarda kablolu ağın yerini almaya başlamıştır. Kablosuz Ağların yaygınlaşması ile kablosuz ağlara bir den çok saldırı tekniği ile saldırılar denenmeye başlanmıştır. Bunlardan en önemlileri şifreleme anahtarlarını kırma ve DoS ataklarıdır. Bu saldırılara karşı önlemler, güvenlik politikaları ve şifreleme algoritmalarındaki gelişmeler bu açığı kapatmaya çalışmaktadır.

1.1 Kablosuz Ağlar

Kablosuz ağlar, kablosuz haberleşme yeteneğine sahip (802.11, bluetooth, infrared, GSM vb.) cihazların herhangi bir fiziksel bağlantı olmaksızın birbirleriyle bağlantı kurmalarını sağlayan ağ yapılarıdır. Kablosuz ağ teknolojisinin kullanım alanları gün geçtikçe artmaya başlamıştır fakat tarihçesi çok eskilere dayanmaktadır. Bu

gelişmeler aslında kablosuz iletişimdeki gelişmeler olarak da kabul edilir. Bunları maddeler halinde listelersek;

- 1831'de Faraday elektromanyetik indüklenmeyi buldu.
- 1864'de J. Maxwell elektromanyetik alan teorisi ve dalga denklemlerini öne sürdü.
- 1888'de Hertz dalgaların uzayda elektriksel olarak yayılımını keşfetti.
- 1896'da Guglielmo Marconi ilk kablosuz telgraf sistemini geliştirdi.
- 1927'de İngiltere ve Amerika arasında ticari olarak ilk radyo telefon servisi geliştirildi.
- 1946'da St. Lous' de bas-konuş teknolojisi kullanılarak ilk araba temelli mobil telefon sistemi kuruldu.
- 1950'de 2400 telefon devreleri destekli ilk karasal mikro dalga telekomünikasyon sistemi TD-2 kuruldu.
- 1960s yüksek güç kapasiteli faklı kanallı veri alıp gönderen bir mobil telefon sistem (IMTS) simülasyonu ile birlikte geliştirildi.
- 1962'de ilk komünikasyon sistemi Telstar yörüngeye yerleştirildi.
- 1964'de INTELSAT uluslar arası telekomünikasyon uydu çalışma grubu Earlybird uydusunu yayınladı.
- 1968'de internetin babası olan Arpanet araştırmalarında kablosuz iletişim üzerine ilk savunma amaçlı gelişmeler yapıldı[Dubendorf V.,2003].

Yukarıdaki listelediğimiz kablosuz iletişimdeki gelişmeler sonucunda 1971 yılında aslında günümüzdeki kablosuz ağların atası gibi kabul edilen ALOHANET ağı kurulmuştur. Bu tarih kablosuz ağ için milat kabul edilir. Şöyle ki İkinci Dünya Savaşında Amerika Birleşik Devletleri ordusu veri transferi için ilk defa radyo sinyallerini kullanmıştır. Çok ciddi bir şifreleme kullanan bir radyo dalgaları ile veri transferi teknolojisi geliştirmişlerdir. Bu teknoloji Amerika ve müttefikleri tarafından savaş sırasında oldukça fazla kullanılmıştır. Bu gelişme 1971 yılında Hawaii Üniversitesindeki bir grup araştırmacıya ilham kaynağı olmuş ve ilk paket tabanlı radyo iletişim ağını kurmalarını sağlamıştır. Adı ALOHANET olan bu ağ, bilinen ilk kablosuz yerel iletişim ağı (WLAN- Wireless Local Area Network) olmuştur. Bu ilk WLAN çift

yönlü yıldız topolojisini kullanan 7 bilgisayardan oluşuyordu. ALOHANET bünyesindeki bilgisayarlar dört ayrı Hawaii adasında yerleşik durumda idi, merkez bilgisayar Oahu adasında bulunuyordu. İşte kablosuz ağın doğuşu bu gelişme kabul edilir. Bunun sonucu olarak gelişmeler yıllar arasında devam etmiştir [Wireless Networks,2008].

- 1973 kısa temel bant iletişimi (UWB – ultra wide band)
- 1979 Nordic kablosuz Telefon Sistemi (NMT)
- 1981'de Global Speciale Mobile (GSM)'in başlaması
- 1982 American Advanced Mobile Phone System (AMPS) çalışmalarının başlaması
- 1984'de CT–1 (Europe) kablosuz telefonlar için standartların belirlenmesi
- 1991'de Digital European Cordless Telephony (DECT)
- 1992'de GSM'in başlaması 215 10 10
- 1994'de Ericsson ilk Bluetooth'u tanıttı.
- 1996'de High Performance Radio Local Area Network (HiperLAN)
- 1997'de Wireless LAN standardı IEEE802.11 Legacy sürümü yayınlandı.
- 1998'de Universal Mobile Telecommunication System (UMTS) IMT–2000 önerisini sunuldu.
- 1998'de Ericsson, IBM, Intel, Nokia, Toshiba farklı protokoller kullanan aygıtların sorunlarını engellemek için tek bir platformda birleşti.
- 1999'da yeni kablosuz LAN standartları – 802.11b ve 802.11a yayınlandı.
- 2000'de yüksek veri iletim hızları ile GPRS denemeleri yapıldı.
- 2000'de 802.11b temelli kablosuz ağ kullanımı popüler oldu.
- 2000'de WEP (Wired Equivalent Privacy) şifrelemesi kırıldı.
- 2001'de 3.Nesil telefonların çalışmalarının başlandı.
- 2001'de Kablosuz geniş bant standardının belirlenmesi IEEE 802. 16 (WiMax)

- 2003'de IEEE 802.16a geliştirilmiş wimax sürümü yayınlandı.
- 2003'de IEEE802.11g sürümü yayınlandı.
- 2003'de IEEE 802.15.4 standardı yayınlandı(ZigBee).
- 2008'de IEEE 802.11n standardı yayınlandı.

Teze başlanıldığında (2007 yılında) iletişim teknolojilerinde ve bilgisayar ağlarındaki hâkimiyet kablolu yerel iletişim ağlarınındı. Fakat son dört senelik bir süreç içerisinde kablosuz yerel iletişim ağlarında aynı zamanda geniş alan ağlarında kullanılan kablosuz iletişim teknolojilerindeki gelişmeler sayesinde kablosuz ortamlar ve iletişim çok yaygınlaşmıştır. Bunun sebeplerini aşağıdaki maddeler altında toplayabiliriz;

- Kablolu iletişim teknolojilerine yakın iletişim hızı
- Kablolu iletişim alt yapısının maliyetinden kurtulma
- Kablodan bağımsızlık, serbest dolaşım
- Kablolu iletişime uygun olmayan yapılarda kullanım
- Kurulum kolaylığı.
- Genişletilebilirlik.
- Kablolu ağ ile bütünleşme

1.2 Kablosuz Ağların Kullanım Alanları

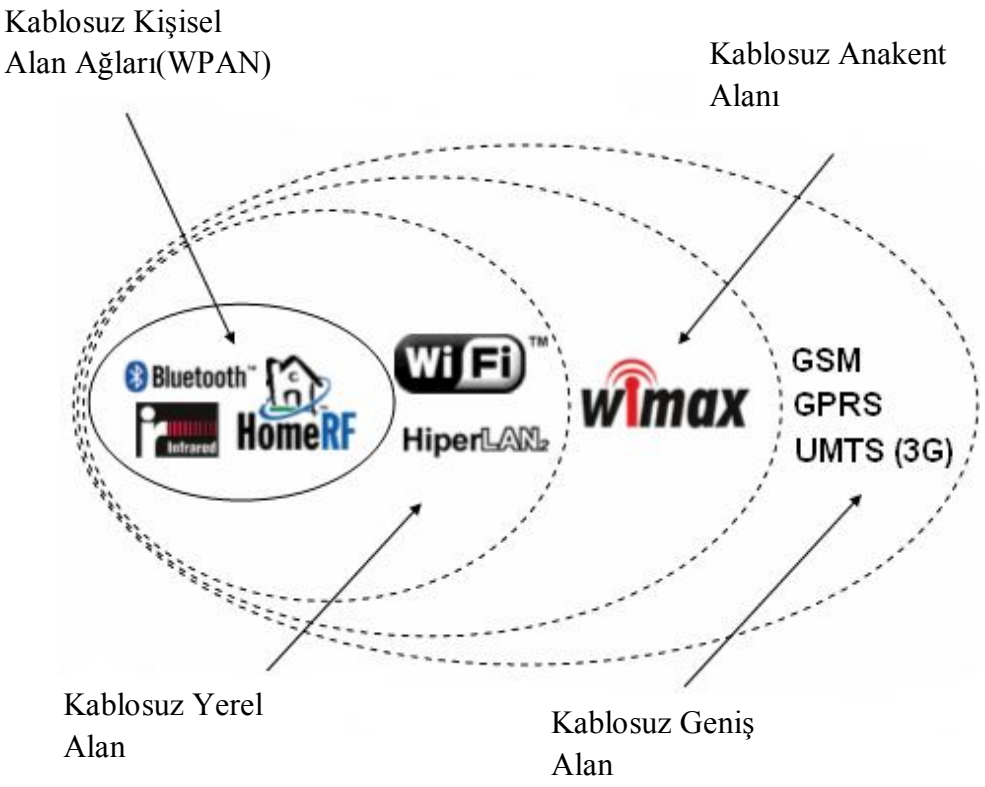
Kablosuz ağlardaki gelişim sayesinde kablosuz ağların kullanım alanları artmıştır. Bu kullanım alanlarından önemli görülenlerden bazılarını şöyle sıralayabiliriz:

- Tarihi eserlerin çok olduğu ortam ve yapılarda kullanılmaktadır. Buna örnek İzmir'in Selçuk ilçesindeki Efes Antik Kentte yapıları bozmadan internet erişimi yapılmaktadır.
- Öğrenci Pansiyonları, Kafe, Eğlence yerleri, restoran, otel gibi geçici hizmet veren yerlerde kullanılmaktadır.

- Devamlı seyahat eden şirketlerde (Şantiyeler için) kullanılmaktadır.
- Akademik ortamlar (konferans) , üniversitelerde kampüsler arası iletişimde kullanılmaktadır.
- Fabrikalarda, satış yerlerinde bar kod cihazlarının etiketlemede (el terminalleri, depolar) kullanılmaktadır
- Cep telefonlarının artık kablosuz iletişime destek vermesi sonucunda cep telefonu yardımıyla İnternete bağlanılmakta kullanılmaktadır.
- Gezgin sağlık bakım profesyonellerine veri iletme gereksinimini olan hastanelerde kullanılmaktadır [Aravamudhan L.,2003 ,Goldsmith A.,2006].

1.3 Kablosuz Haberleşme Teknolojileri Ve Türleri

Kullanım alanlarına, iletişim gücüne ve kapsama alanına göre kablolu ağlardaki ağ tipleri gibi kablosuz ağlarda da kullanılan teknoloji ve türler sınıflandırılmıştır. Yerel alan ağlarda (LAN-Local Area Network) kullanılan kablosuz olarak oluşturulan yerel ağlar için WLAN ismi kullanılmaktadır. Ayrıca kullanılan kablosuz ağ standartları her ortam için bazı ölçütlere göre farklıdır. Bu ağ yapıları aşağıdaki şekilde görülmektedir.



Şekil 1. 1. Kablosuz Ağ Kategorileri [Wireless Networks,2008]

Günümüzde kullanılan kablosuz ağlar için standartlar IEEE (Institute of Electrical and Electronical Engineers) tarafından belirlenmektedir.

1.3.1 IEEE (Institute Of Electrical And Electronical Engineers) Standartları

IEEE, bilim dünyasında, mühendisliğin yaratıcılık, geliştirme, bütünleştirme, paylaştırma işlevine, elektro teknoloji ve bilgi teknolojisine, insanlığa yararlı bilimlere ve uzmanlık alanlarına katkıda bulunan kar amacı olmayan teknik bir mesleki organizasyon olarak bilinmektedir.

AIEE (American Institute of Electrical Engineers) ve IRE (Institute of Radio Engineers) topluluklarının birleşmesi ile 1963 yılında resmen kurulan IEEE, dünya genelindeki en büyük teknik organizasyonlardan birisidir. 2007 yılı itibariyle 160

ülkede 375.000'den fazla üyesi bulunan enstitünün üyelerinin yüzde 35'i ABD dışında yaşamaktadır. IEEE tüm dünyada Elektrik-Elektronik ve Bilgisayar Mühendisliği yayınlarının yaklaşık yüzde 25'ini tek başına yayınlamakta ve birçok elektronik cihazın standartlarını belirlemektedir.

IEEE, 802.X adı altında IEEE, yerel ağlar metrapol ağlar ve kişisel ağlar için standartlar oluşturmuştur. Standart komitesi kendi içinde 802.1 den 802.17 ye kadar çalışma gruplarına ayrılmıştır. Bu çalışma gruplarına ayrılmanın sebebi her grubun farklı konular üzerinde gelişmeler sağlaması içindir. Böylece tüm yük bir komite üzerinde olmayıp görev dağılımı yapılmıştır. Bilinen IEEE çalışma grupları:

- 802.1 Güvenlik ve Diğer Konular
- 802.3 Ethernet Çalışma Grupları
- 802.11 Kablosuz Yerel Ağlar
- 802.15 Kablosuz Kişisel Alan Ağları Çalışma Grubudur.

Yukarıdaki çalışma grupları çok bilinen aktif çalışma gruplarıdır. Fakat IEEE 802 çalışma grupları sadece yukarıdaki maddelendirdiğimiz çalışma gruplarıyla sınırlı değildir. Bunlara ek olarak kablosuz ağlarla ilgili IEEE 802.1X ve 802.2X çalışma gruplarının tablo 1. 1.'de listesi verilmiştir.

Standart	Açıklama
802.11	Kablosuz Yerel Alan Ağları Orijinal Standardıdır
802.15	Kablosuz Kişisel Alan Ağları Çalışma Grubudur
802.16	Geniş Bant (Broadband) Kablosuz Erişim Çalışma Grubu
802.18	Radyo Sinyali Düzenleyici Çalışma Grubu
802.19	Kablosuz Koekzistans Çalışma Grubudur
802.20	Mobil Geniş Bant Kablosuz Erişim Çalışma Grubu
802.22	Kablosuz Bölgesel Alan Ağları Çalışma Grubudur

Tablo 1. 1. IEEE 802 Kablosuz Ağlar Çalışma Grupları

[IEEE 802 Working Group,2011]

1.3.2 Kablosuz Kişisel Alan Ağları (WPAN-Wireless Personel Area Network)

Kablosuz kişisel alan ağları, kısa mesafeli radyo frekansı teknolojileri kullanarak kurulan ağlardır. Genellikle kablosuz yazıcı, cep telefonu, PDA ve birbirine yakın iki bilgisayar arasında bu ağ kurulur. Günümüzde en çok kullanımı cep telefonları arasında ya da cep telefonları ile dizüstü bilgisayar arasında müzik, resim, medya paylaşımı içindir. Bu ağlarda birkaç teknoloji kullanılır. Bunlar Bluetooth, HomeRf, IrDA, ZigBee teknolojileridir[Borsc M.,Shinde H.,2005].

1.3.2.1 IEEE 802.15 Standardı

1999 Mart ayında 802 yerel ve ana kent alan standardı komitesi IEEE bilgisayar birliğinin bir bölümü 802.15 çalışma grubunu oluşturmuştur. 802.15 çalışma grubu WPAN yani kablosuz kişisel alan ağları diye bilinen kısa mesafeli kablosuz ağlar için özel gelişme standartları ile kurulmuştur. Tablo1.2'de bu standardların listesi verilmiştir.

Proje	**Veri Hızı**	**Mesafe**	**Configirasyon**	**Diğer Özellikler**
802.15.1 (Bluetooth)	1 Mbps	10M (sınıf 3) 100M (sınıf 1)	8 Aktif Aygıt Piconet/Scatternet	Kimlik Doğrulama, Ses, Şifreleme
802.15.2 Koekzistans	Yeni Bir Model ve Mekanizmalar Geliştirmek Pratikleri Sağlayan Dokümanlar			
802.15.3 Yüksek Hız	22, 33, 44, 55Mbps	10M	256 Aktif Aygıt Piconet/Scatternet	
802.15.4 ZigBee	250 Üzerinde /kbps	10M Normal 1M-100M Ayarlara Bağlı	Efendi/Köle (256 Aygıt ve Daha Fazlası) Noktadan Noktaya	Pil Süresi: Aylarca Bitmez
802.15.5 Mesh WPAN	Mesh Kablosuz Kişisel Alan Ağları İçin Geliştirilen Standart			
802.15.6	Daha Standartlaşmamış Body Area Network (BAN) Çalışma Grubu			

Tablo 1. 2. IEEE 802.15 Standartları[Tjensvold M.,2007]

IEEE 802.15 grubu içinde dört adet görev tanımlaması yapılmıştır.

- Birinci görev grubu Bluetooth teknolojisine dayalı WPAN standartları geliştirmek için sorumlu tutulmuştur. Operasyon aralığı (POS-Personal operating space) 10 metreye kadar her yönde genişleyebilir sabit ya da taşınabilir WPAN aygıtlarıdır.

- İkinci görev grubu mümkün olabilecek minimum parazitle WPAN ve WLAN ağ tiplerini aynı ortamda çalıştırmadan sorumlu tutulmuştur.

- Üçüncü görev grubu yüksek hız WPAN standartlarını geliştirmeden sorumlu tutulmuştur. Beklenen minimum değer oranı ise 20 Mb/s'dır. Buradaki amaç geniş hacimli verilere sahip olan uygulamalar arasında veri transferidir.

- Dördüncü görev grubu düşük hız WPAN standartlarını geliştirmeden sorumlu tutulmuştur. Beklenen maksimum değer oranı ise 200 kb/s'dır. Buradaki amaç pille çalışan aygıtları uzun yıllarca şarj etmeden çalışabilir tutmaktır.

1.3.2.2 Bluetooth (IEEE 802.15.1)

Bluetooth[1], cihazların düşük hızda bire bir haberleşmeleri için kullanılan, genellikle kısa menzilli (10 ile 100 metre) kablosuz haberleşme sistemleridir. Bluetooth

[1] Danimarka ve Noveç'in Viking kralı Harald Gormsson'nin "Blatand" lakabından adını almıştır. Kralın dişlerinin bir diş hastalığı yüzünden maviye döndüğüne inanılır bu yüzden mavi diş olarak bilinir.

haberleşmesi 802.11b/g ile aynı frekans bandında (2.4 GHz-ISM) gerçekleşmektedir, bu sebeple Bluetooth haberleşmeleri 802.11b/g haberleşmeleri üzerinde gürültü olarak olumsuz etki yapabilmektedir. Bluetooth haberleşmesi için cihazlar arasında direk görüş hattı (LOS-Line of Sight)olmasıgerekmemektedir [Bluetooth Haberleri,2008].Bluetooth teknolojisi zaman içerisinde çok gelişme gösterdi ve birçok sürümü yayınlandı. Bunlar şunlardır:

Bluetooth 1.2 = 721Kbit/s

Bluetooth 2.0 = 2Mb/s

Bluetooth 2.0 EDR = 3Mb/s

Bluetooth 2.1 = 784kbit/s

Bluetooth 3.0 = 24 Mbps

Bluetooth 4.0 = 24 Mbps

Günümüzde Bluetooth 3.0 ve 4.0 artık kullanılmaya başlanmıştır. Eskiye dönük çalışabilmelerinin yanında yüksek veri hızı ve güvenlik geliştirilmiştir. Şu an aktif olarak çoğu cep telefonunda ve diz üstü bilgisayarda Bluetooth 3. 0 sürümü kullanılmaktadır.

Bluetooth 3.0'ın özelliklerini detaylandırırsak;

- Kablosuz bağlantı hızı yaklaşık olarak 24 Mbps'dir.
- Senkronize olurken bağlantı kopukluğu yaşanma ihtimali oldukça azdır.
- Generic Alternate MAC/PHY (AMP) teknolojisi mevcuttur.
- Aygıtların Wi-Fi hızı ile veri aktarması sağlanabiliyor. (802.11 teknolojisi ile)
- Ucuzdur. Hatta ücretsiz denebilir.
- Enerji tüketimi oldukça azdır.
- Enhanced Power Control özelliği ile kulaklık ve cep telefonu arasında kablosuz bağlantı kesilmesi durumunu ortadan kaldıracak nitelikte olması.

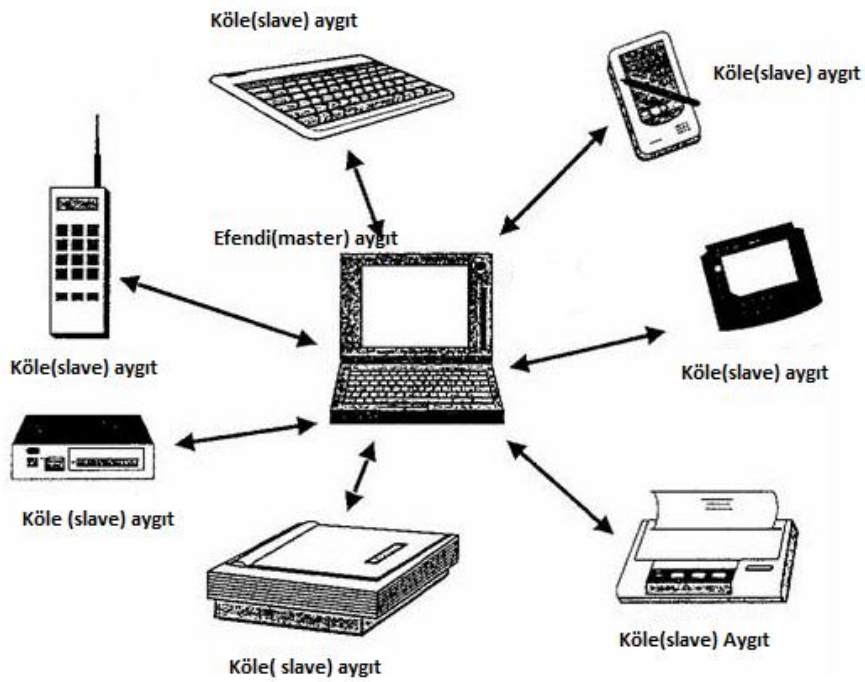
Bunun yanında 4.0 sürümü ile göze çarpan yenilik, güvenlik için AES 128 bit güvenliğin kullanılmasıdır. [Bluetooth 3.0-4.0,2010]

Bluetooth haberleşmesine örnek olarak;

- Bilgisayarların düşük hızlı kısa mesafeli haberleşmeleri
- Cep telefonları arasında ve PC'ye veri transferi
- Bluetooth kulaklık
- Bluetooth ile yazıcı kullanımı verilebilir.

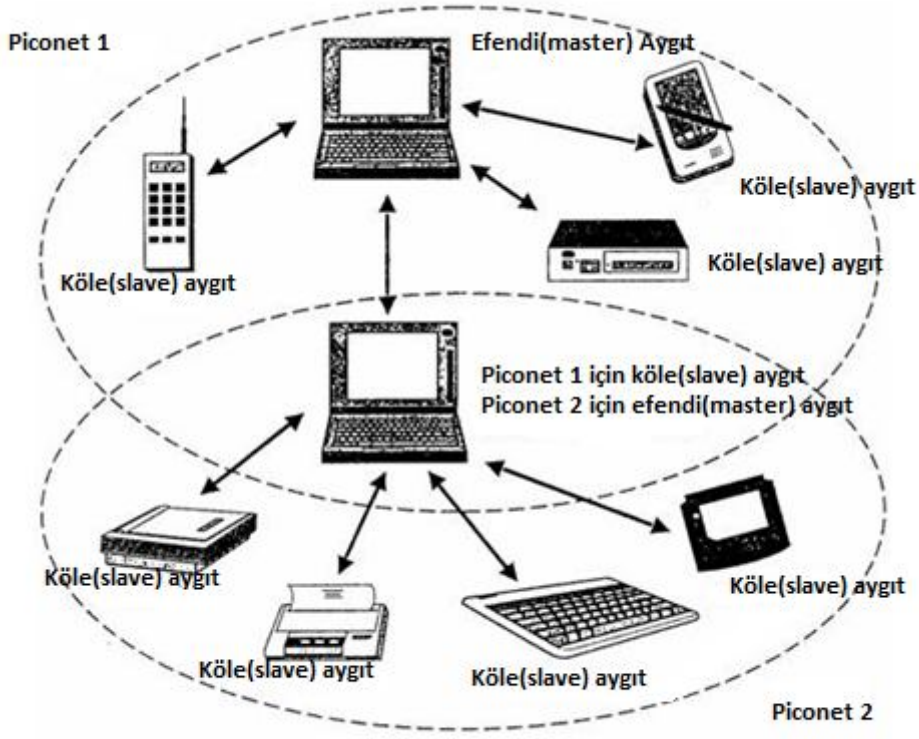
Bir Bluetooth WPAN maksimum sekiz aktif aygıt içerebildiği görülür. Bu tip ağlar genelde piconet olarak isimlendirilir.

Piconet içindeki bir aygıt master(efendi) olmak için tasarlanır, diğer aygıtlar ise slave(köle) olarak tanımlanır. Herhangi Bluetooth aygıtı efendi ya da köle olabilir. Genel piconet üzerine tasarlanmış aygıtlar efendi olarak belirlenir. Efendi aygıtın gerçek rolü aygıtlar arası eşleme sağlamak ve kontrol etmektir. Bir piconet 7 aktif köleden oluşabilir.



Şekil 1. 2. Bluetooth Piconet Yapısı [Kablosuz Teknoloji,2005]

Ofis gibi çoklu kullanıcı ortamlarında birden fazla piconet aktif olabilir. Scatternet, kavramı 2 veya daha fazla piconet'in aynı ortamdaki topluluğunu anlatır. Bu tür durumlarda tek bir bluetooth aygıtı birden fazla piconet üzerinde efendi ya da köle olarak aktif olabilir. Bu yapılar teoride gösterilen yapılardır. Fakat Bluetooth ile ofislerde böyle yapılar yerine Wi-fi(Wireless Fidelity) teknolojisi kullanılır. Bluetooth daha çok anlatıldığı gibi kısa mesafede bilgisayar ile özellikle cep telefonları arasında multimedya, resim, dosya transferi için çok kullanışlıdır.



Şekil 1. 3. Bluetooth Scatternet Yapısı [Kablosuz Teknoloji,2005]

1.3.2.3 HomeRF

HomeRF, ev ve küçük işyerleri için geliştirilen kablosuz erişim standardıdır. Özellikleri Mart 1998'de kurulan Ev Radio Frekans Çalışma Grubu (HomeRF WG-

Home Radio Frequency Working Group) isimli çalışma grubu tarafından ortak kablosuz erişim protokolü (SWAP-Shared Wireless Application Protocol) adı altında duyurulmuştur. HomeRF evde bulunan kişisel bilgisayar, kordonsuz telefon ve diğer cihazlar arasında ses ve veri iletişimini kablolama masrafına gerek kalmadan kablosuz olarak sağlamaktadır. [HomeRf,2002]

HomeRF Çalışma Gurubunun kurulmasından sonra pek çok firma bu guruba katılmış ve üye sayısı 100 civarına ulaşmıştır. Son olarak her biri kendi sektöründe lider konumda olan Compaq, Intel, Motorola, National Semiconductor, Proxim ve Siemens firmalarının katılımıyla çalışmalar sonuçlandırılarak SWAP 2.0 geliştirilmiştir. SWAP 2.0 ile başlangıçta 1.6 Mbps olan veri iletişim hızı 10 Mbps'e çıkarılmıştır. Gelecekte veri iletişim hızının 20 Mbps veya daha yükseğe çıkarılması hedeflenmiştir [Kaminski,2001]. HomeRF sistemi 2.4 GHz ISM bandında çalışmakta ve 50 metreye kadar mesafede veri iletişimi sağlamaktadır. HomeRF 2.0 sistemlerinde FHSS modülasyon tekniği kullanılmaktadır. FHSS modlüsyan tekniği bu tezde ileri ki bölümlerde anlatılmaktadır. HomeRF aynı frekans bandını kullanan WLAN sistemleri tarafından karışıma maruz bırakılmaktadır. Ancak Bluetooth teknolojisi tarafından karışım verilmez. Çünkü HomeRF kullanıldığı FHSS tekniği saniyesinde birbirine girişim yapmayan 15 frekans kanalına sahiptir.

1.3.2.4 IrDA (Infrared Data Association)

IrDA, yönlü ışık demeti aracılığıyla ışığın dalga yapısı sayesinde kızılötesi (infrared) frekanslarda gerçekleştirilen kablosuz iletişim teknolojisidir. Alıcı ile verici cihaz arasında açık görüş hattının bulunduğu ortamlarda ve kısa mesafeler için çok uygundur. Kızılötesi teknolojisini iki tür kullanmak mümkündür. Birincisi görüş hattı (direct beam, line of sight), ikincisi ise yansıma (diffused beam) yöntemidir [Geier J.,2002 ,Patil B.,2003]. Doğal olarak görüş hattı yöntemi diğerine oranla daha fazla veri

iletişimi sağlamaktadır. Ancak uygulama da geniş alan kaplamak ya da çok kullanıcıya ulaşabilmek için yansıma yöntemi tercih edilmektedir. Kızılötesi teknolojisi büyük oranda uzaktan kumanda cihazlarında kullanılmaktadır. 16 Mbps veri hızlarındaki uygulamaları yaygın olarak kullanılmakta olan kızılötesi iletişim teknolojisi, Infrared Data Association tarafından, 100 Mbps düzeyinde multimedya uygulamalarını destekleyecek hale getirilmeye çalışılmaktadır[Infrared,2011].

IrDA'nın üstünlükleri:

- Serbest kullanıma açıktır. Bir lisans ve ücret gerektirmez.
- RF sinyallerinden etkilemez.
- Güç tüketimi düşüktür.
- Kapalı ortamlarda yetkisiz dinlemeye ve bozucu etkilere karşı tam bir güvenlik sağlar.

IrDA'nın zayıflıkları:

- İletişim mesafesi kısadır. İdeal şartlarda 10-15 metredir.
- Sinyaller katı cisimleri geçemez. Bu sebeple kapalı alanlarda duvar, kapı ve büro malzemeleri tarafından kullanım için uygundur.
- Sinyaller kar, sis, toz ve ışık gibi hava şartlarından etkilenir.
- Bu sebeple açık alanlarda kullanım için uygun değildir.
- Kirlilik sinyalleri etkiler.

1.3.2.5 ZigBee (IEEE 802.15.4)

Kablosuz Sensör Ağlar (WSN-Wireless Sensor Networks) endüstride günümüzün en etkileyici teknolojilerinden biridir. Kablosuz bağlanabilirlik için yeni bir standart olan ZigBee[2], IEEE tarafından duyurulan IEEE 802.15.4 standartını temel alır ve ZigBee Alliance ilk genel standartını uygulamalarda kullanılmak üzere sağlamıştır. ZigBee Alliance; Ivensys, Honeywell, Mitsubishi Electric, Motorola ve Philips gibi 200 kadar firmadan oluşmaktadır[IEEE,2008].

Güvenilir olması, düşük maliyeti ve enerji tasarrufu gibi avantajları göz önüne alındığımızda ZigBee, PC girdi aygıtları gibi sensör ve yönetim ürünlerinin kablosuz bağlantıları için kullanılabilmektedir. ZigBee, kablosuz iletişim kanallarının otomatik olarak aranmasına ve çok sayıda kablosuz ağın bir arada var olmasına imkân tanımaktadır.

ZigBee teknolojisi ürünleri, dünya çapında kullanıma açık olan 2.4 GHz frekans bandını kullanmaktadır. Buna ek olarak, Amerika kıtasında 915 MHz ve Avrupa'da 868 MHz de kullanılabilmektedir. 2.4 GHz frekansında on kanal ile 250 kbps, 915 MHz frekansında altı kanal ile 40 kbps ve 868 MHz frekansında bir kanal ile 20 kbps hızlarına erişilebilmektedir. Ürünlerin erişim mesafesi iletim gücü ve çevre etkilerine bağlı olarak 10 ile 75 metre arasında değişmektedir.

ZigBee'nin amacı sık kullanılmayan ama uzaktan kullanımı da gerekebilen cihazlara ya da nokta algılayıcılara bir kablosuz ağ protokolü sunmaktır. ZigBee'nin bu konudaki en tanınmış rakibi Bluetoothtur. Fakat iki teknoloji aynı pazara hitap etmediklerinden karşılaştırma çok yapılmamıştır. ZigBee Bluetootha göre 1/6 hızında

---

[2] ZigBee ismini, arıların çiçekten çiçeğe dolaşırken izledikleri zig-zag şeklindeki yoldan almıştır. Bu dolaşım sırasında, diğer arıların bu kaynaklara (çiçeklere) nasıl (nereden) ulaşmış oldukları bilgisiyle hareket ederler.

fakat kapsama alanı bluetootha göre daha fazladır. En önemli farkı ise inanılmaz az enerji harcaması ve büyük olasılıkla tekrar şarj edilmeyecek piller ile kullanılacak olmasıdır. ZigBee'nin kullanım alanı, ev aygıtlarından, arabaların çeşitli parçalarına kadar birçok yer olabilir. Sonuçta size bilgi gelmesini isteyeceğiniz her nokta ZigBee için uygun bir sistemdir. Ayrıca kablosuz ve ucuz olduğundan kablolama maliyetlerini de düşürebilir. Hatta bazı sürümleri kendi enerjilerini üretecek şekilde bile tasarlanabilir[ZigBee Alliance, 2011]. ZigBee teknolojisi IEEE 802.11b ve Bluetooth'dan daha yavaştır. Fakat daha az güç ile ve farklı alanlarda çalışmaktadır. [Safaric S. ,Malaric K.,2006]

ZigBee'nin diğer kablosuz iletişim ağları ile karşılaştırılması aşağıdaki tabloda gösterilmektedir.

	ZigBee	**GPRS/GSM**	**Wi-Fi**	**Bluetooth**
Odaklanma Alanı	İzleme ve Kontrol	Geniş Alan Ses ve Veri	Web, Email, Video	Kablo Yerine
Sistem Kaynağı	4–32 Kb	16 MB+	1 MB+	250Kb+
Pil Ömrü(Gün)	100- 1000+	1–7 Gün	0.5- 5	1–7
Ağ Boyutu	Sınırsız 2^{64}	16 Mb+	32	7
Ağ Veri Genişliği (kb/sn)	100- 1000+	64- 128+	11000- 54000	720
Kapsama Alanı (Metre)	1–100+	1000+	1–100	1–10+
Başarı Alanları	Dayanıklılık, Maliyet, Güç Tüketimi	Ulaşulabilirlik, Kalite	Hız, Esneklik	Maliyet, Rahatlık

Tablo 1.3. ZigBee İle Diğer Kablosuz Teknolojilerin Karşılaştırılması

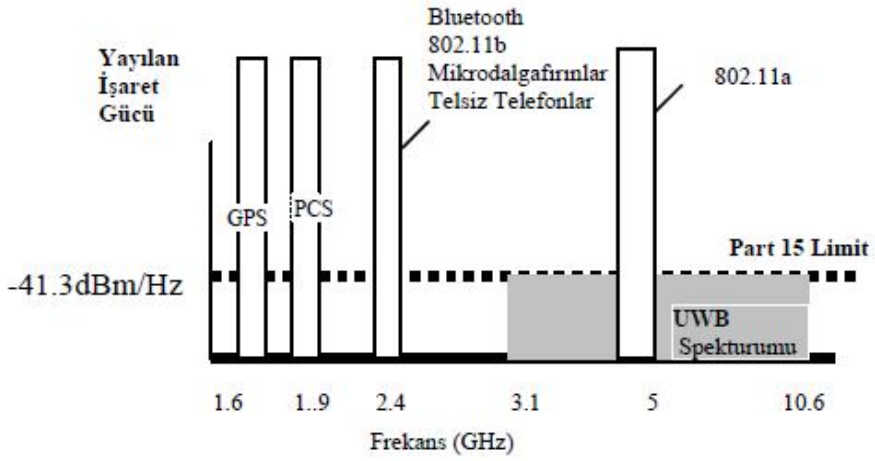
1.3.2.6 Uwb (Ultra Wideband–802.15.3a)

UWB teknolojisi, altyapısındaki kapasite açısından, bir POS alan içerisinde 800 MBps düzeylerine kadar veri hızı destekleyebilecek olanakta olup temelde WiMedia uygulamaları için geliştirilmektedir. Kablolu iletişim hızlarını kablosuz bir teknoloji

olarak sunmayı hedefleyen ve uzun pil ömrünü desteklemeyi amaçlayan UWB, ev ağ oluşumu, multimedya veri iletimi, radar teknolojileri, kablosuz intercom gibi uygulamalar için çözüm sunmaktadır. UWB sinyali genliğin -10 dB noktasında ölçülen frekans bandının merkez frekans değerinin %20'sinden daha büyük ya da RF bant genişliği 500MHz den daha fazla olan sinyallerdir. UWB 4G nesil sistemlerin ihtiyacı olan geniş bant ihtiyacını kolaylıkla sağlar. UWB son yıllarda araştırmacıların ve endüstrinin üzerinde çalıştığı yeni nesil kablosuz kişisel ağ teknolojisidir. UWB teknoloji 7.5 GHz gibi aşırı bant genişliğini, kısa mesafede düşük güç ile kullanır. IEEE 802.15.3a grubu UWB teknolojinin standardını oluşturmaktadır. Oluşturulan standart için hedef 10 m mesafede ise saniyede 110 Mega bit veri iletim hızına, 4 m mesafede ise saniyede 200 megabit veri iletim hızına çıkılmasıdır [Molish F.,2003]. Daha düşük mesafelerde daha yüksek veri iletim hızları hedeflenmektedir.

Uzaysal kanal kapasitesi bakımından (birim kare başına birim saniyedeki bit sayısı, bit/s/m^2) IEEE 802.11 ve Bluetooth gibi diğer kısa mesafe kablosuz teknolojilerinden daha üstün performans göstermektedir. Araştırmacılar tarafından sunulan iki çeşit UWB tekniği mevcuttur. Birincisi Doğrudan Dizili Ultra Genişbant (DS-UWB) diğeri ise Dik Frekans Bölmeli Çoklama (OFDM) tekniğidir. DS-UWB tek taşıyıcılı bir teknik olmasına karşın OFDM çoklu taşıyıcılı bir tekniktir. Bu teknik ileriki bölümlerde anlatılmıştır. UWB tamamen sayısal bir haberleşme sistemi olduğu için Darbe Konum Modülasyonu (PPM), Darbe Genlik Modülasyonu (PAM) ve Var/Yok Anahtarlaması (On/Off Keying, OOK) gibi temel bant sayısal modülasyon teknikleri kullanır.

UWB sinyalinin güç spektral yoğunluğu incelendiğinde düşük güç seviyelerinde olduğu görülür. Bu özelliği sayesinde mevcut dar bant sinyallerine karışım vermez[Kim Y.,2003].



Şekil 1. 4. Kuzey Amerika UWB Spektrumu
[UWB Data Transfer Tecnology,2007]

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

WLAN, bir bina, okul, hastane, kampüs gibi sınırlı bir coğrafi alanda kurulan ve çok sayıda kişisel bilgisayarın yer aldığı ağlardır. WLAN'lar, kamu kurum ve kuruluşlarında, şirketlerde, üniversitelerde, konferans salonlarında ve benzeri pek çok yerde kullanılmaktadır. WLAN'larda bilgisayarlar ve ağ içerisindeki diğer cihazlar arasında iletişimi sağlamak üzere kablo yerine Radyo Frekansı (RF-Radio Frequency) veya kızılötesi teknolojisi kullanırlar. 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[Geier J.,2006 ,Matthew S.,2005].

1.3.3.1 IEEE 802. 11 Standardı

IEEE, 802'yi yerel alan ağı standartlarını, 802.11'i kablosuz yerel alan ağlarını, sonunda bulunan a, b, g, n gibi harfler ile özelleşmiş kablosuz ağ standartlarını tanımlamak için kullanmaktadır. Bu standardlar farklı gelişmeler ve üstünlükler anlamına gelmektedir.

IEEE 802.11 b,g, Türkiye'de 2. 4 GHz ISM radyo frekans bandında yüksek hızlı veri transferinin mümkün kılmaktadır. (802.11b ile 11Mbps, 802.11g ile 54 Mbps). Kapsama alanı 10 ila 100 metre arasında değişen (anten, alıcı kazancı, sinyal gücü, ortam gibi değişkenlere bağlı olarak), dizüstü bilgisayar, masaüstü bilgisayar, PDA vb. cihazların bir erişim noktası üzerinden ya da birbirleriyle kurdukları direk bağlantı ile haberleşmelerini sağlayan kablosuz ağ yapılarıdır. Kablosuz Ethernet ya da Wi-Fi (Wireless Fidelity) olarak da adlandırılmaktadır. IEEE 802.11a [IEEE,2007], avrupa dışında kullanılan, 802.11b,g standardından farklı olarak 5. 0 GHz ISM bandında veri transferine izin veren standarttır. Türkiye'de kullanımına izin verilmemektedir. Son gelişen standard olarak öne çıkan IEEE 802.11n, çoklu antenler ve çeşitli protokoller kullanarak maksimum veri transfer hızını 540 Mbps'a çıkaran standarttır. Bu standartlar ileriki bölümlerde ayrıntılı olarak incelenecektir.

1.3.3.2 HiperLAN

Yüksek Performanslı Radyo Yerel Ağı (HiperLAN-High Performance Radio LAN), ETSI tarafından tanımlanmış, OFDM kodlama ve modülasyon yöntemi kullanılan, 5 GHz bandında çalışan kablosuz LAN standardıdır. HiperLAN1, HiperLAN2 olmak üzere 2 tipi vardır. HiperLAN2, ETSI (Europan Telecominications Standarts Institute) ve Hiperlan2, Global Forum (Bosh, Nokia, Ericson, Dell, Telra ve

Texas Instruments gibi firmalar öncülüğünde kurulmuş bir şirketler birliği) tarafından geliştirilmiştir. IEEE 802.11a standardına rakiptir ve 54Mbs'ı 5.4 GHz'de iletir. HiperLAN2 esas olarak 802.11a'nın rakibi ve Avrupa' da yaygın olarak kullanılan bir standarttır. HiperLAN2 ve 802.11a aynı 5 GHz'lik bandı kullanırlar ve her ikisi de 54Mbps veri aktarımı yapabilirler. [ETSI,2004]. 802.11a özellikle çoklu ortam (multimedia) uygulamalarını kısıtlarken, HiperLAN2 daha pahalı bir sistem olmakla birlikte yüksek veri oranlarıyla resim ve görüntü aktarımında daha iyi performans sağlamaktadır. HiperLAN'lar ATM teknolojisi esaslıdır ve 802.11 teknolojisinden daha iyi servis kalitesine sahiptir [Eklund C.,Roger B.,Kenneth L.,2002]. HiperLAN2 ağında erişim noktalarından uç sistemlere bağlantıya yönelik bir yaklaşım vardır. Böylece, 802.11 kablosuz LAN uygulamalarının aksine ses ve görüntü aktarımı için gerekli trafik türü desteklenmektedir. 5 GHz ISM bandı Türkiye'de kullanılan bir bant değildir. Fakat ETSI geliştirilen 2 adet tamamlayıcı standart daha oluşturulmuştur. Bu ikisinin isimleri HiperAccess ve HiperMan'dır. Özellikle WMAN ağlarında günümüzde kullanılan WiMAX tekonolojiside 802.16x ve ETSI HiperMAN standartlarına dayandırılmıştır. Bu doktora tezinde HiperLAN teknolojisi üzerinde sadece açıklayıcı bilgi olarak durulmuştur. Bunun yanında son olarak aşağıdaki tablo 'da 802.11a ile HiperLAN2 teknolojisinin karşılaştırılması yapılmıştır.

Özellik	**HiperLAN2**	**802.11a**
Brüt Aktarım Oranı	54 Mbps	54 Mbps
Net Veri Oranı	32 Mbps	32 Mbps
Frekans Bandı	5 GHz	5 GHz
Frekans Seçimi	Tek Taşıyıcı	DFS İle Tek Taşıyıcı
Ortama Erişim	TDMA\TDD	CSMA\CA
Şifreleme	DES,3DES	40 Bit RC4
Modülasyon Yönetimi	OFDM	OFDM

Tablo 1. 4. HiperLAN2 ile 802.11a'nın standartlarının karşılaştırılması

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

WMAN teknolojileri, kullanıcılara anakent alanı içinde çeşitli yerler arasında kablosuz bağlantılar kurma olanağı verir. Buna ek olarak, WMAN'ler, kablolu ağların birincil kiralanmış hatları kullanılabilir olmadığında yedek olarak da hizmet verebilir.

WMAN'ler veri aktarımı için radyo dalgaları veya kızılötesi ısınlar kullanır. WMAN'ler kablolu ağlardan çok daha ucuz, esnek ve kolay kurulum özelliklerine sahiptir[Yang F., Zhou F., Zhang L.., 2005]. Kırsal bölgelerde sabit geniş bant olanaklarını sunmanın güç olduğu yerlerde ya da şehir yaşamında servis veren şirketlerin kendi bölgesel şebekeleri arasında hızlı ve güvenilir haberleşme altyapısı oluşturmasını sağlar. Ancak, bu tür uygulamalar oldukça yenidir ve geliştirme çalışmaları devam etmektedir. Bu alanda, WiMAX adı altında uygulamalar yapılmaktadır.

1.3.4.1 IEEE 802.16 Standardı

IEEE 802.16 standardı Ekim 2001 tarihinde tamamlanmış ve 8 Nisan 2002'de kablosuz anakent alan ağları için geliştirilmiştir. WMAN'lar kablolu erişim ağlarına (fiberoptik, coacxial gibi sistemleri kullanan kablolu ağlara) alternatif olarak telsiz iletişim kullanılarak yüksek miktarda veri iletişimi sağlamak için geliştirilmiştir [Eklund C., Roger B., Kenneth L., 2002]. Kablo alt yapısının olmadığı bütün bölgelerde çalışabilir ve uygulanabilir olmasının yanı sıra mevcut hücresel haberleşme sistemleri ve kablosuz ağ sıcak noktaları ile uyumlu çalışması hedeflenmektedir.[Kavas A.,2006] Bu kablosuz erişim teknolojisi WiMAX olarakda bilinir. Bunun sebebi engebeli alanlarda kablonun pahalılığını ve alt yapı zorluluğunu gidermektedir. IEEE 802.16

standardı, 2 GHz-11 GHz ve 10 GHz-66 GHz geniş bant frekans aralıkların da 120 Mbps veri hızlarına ulaşabilen uygulamaları kapsamaktadır.

1.3.4.2 WiMAX (World Wide Interoperability for Microwave Access)

IEEE 802.16e standardı ile tanımlanmış bir kablosuz geniş bant erişim teknolojisidir. Teorik olarak IEEE 802.16 standardı görüş hattı gerektirmeden 50 km'ye kadar kapsama alanı sağlamak ve maksimum 75 Mbps'lik (yakın mesafelerde) iletim hızını mümkün kılmak üzere tasarlanmıştır. Çeşitli ülkelerde farklılık göstermekle birlikte 2 GHz-11GHz aralığında belirli frekans bantlarının WiMAX Mobil kullanıcılara mekândan bağımsız internet erişimi sunmayı amaçlamakta, ayrıca kablolamanın maliyet ve/veya coğrafi şartlar sebebiyle elverişli olmadığı bölgelerde alternatif bir olarak düşünülmektedir. 2011 yılı itibariyle Türkiye'de pilot uygulamalar yapılmaktadır, fakat henüz etkin olarak kullanılmamaktadır. Kullanımı artıkça, Türkiye'de kullanımda olan T1 ve ADSL'e alternatif olacağı düşünülmektedir[Kavas A.,2006]. Wimax'ın standard özellikleri tablo 1. 5. te verilmiştir.

Bunun yanında WiMAX şebekesine erişim,

- Sabit Noktadan Erişim,
- Göçebe Erişim,
- Taşınabilir Erişim,
- Yarı-Gezgin Erişim,
- Tam Gezgin Erişim

5 farklı şekilde mümkün olacaktır. Özelliklerin karşılatırılması tablo 1.6.'da görülmektedir.

Standart	802.16	802.16a/REVd	802.16e
Standart Yılı	Eylül 2001	802.16a Haziran 2003 802.16REVd Eylül 2004	2005
Frekans Spektrumu	10–66 GHz	<11 GHz	<6 GHz
Haberleşme Özelliği	Doğrudan görüş hattı gerektirir.	Doğrudan görüş hattı gerektirmemekte	Doğrudan görüş hattı gerektirmemekte
Bant Genişliği	28MHz'de 32–134 Mbps	20 MHz'de 75 Mbps	5 MHz'de 15Mbps'a kadar çıkabilir
Modülasyon	QPSK, 16QAM, 64QAM	OFDM256, OFDMA, 64QAM, 16QAM, QPSK, BPSK	OFDM256, OFDMA, 64QAM, 16QAM, QPSK, BPSK
Hareketlilik	Sabit Uygulamalar	Sabit ve taşınabilir uygulamalar	Hareketli uygulamalar
Kanal Bant Genişliği	20, 25 ve 28 MHz	1.25- 20 MHz arasında seçilebilir bant genişliği	1.25- 20 MHz arasında seçilebilir bant genişliği
Hücre Yarıçapı	1.6–5 km	5–8 km Kule yüksekliği, verici gücü ve anten kazancına bağlı olarak 50 km kadar hizmet verebilir.	1,6–5 km

Tablo 1. 5. WiMAX Standart Özellikleri

Erişim Özelliği	Kullanılan Cihaz	Konum/ Hız	Aktarma Özelliği	802.16–2004	802.16e
Sabit Noktadan Erişim	Bilgisayar	Tek/ Sabit	Yok	Var	Var
Göçebe Erişim	Bilgisayar/ Dizüstü Bilgisayar	Çoklu/Sabit	Yok	Var	Var
Taşınabilir Erişim	Dizüstü Bilgisayar	Çoklu/ Yaya Hızında	Sert Aktarma	Yok	Var
Yarı- Gezgin Erişim	Dizüstü Bilgisayar/ PDA	Çoklu/ Düşük Araç Hızında	Sert Aktarma	Yok	Var
Tam- Gezgin Erişim	Dizüstü Bilgisayar/ (PDA)	Çoklu/ Yüksek Araç Hızında	Yumuşak Aktarma	Yok	Var

Tablo 1. 6 WiMAX Erişim Özelliklerininin Karşılaştırılması

1.3.5 Kablosuz Geniş Alan Ağları (WWAN-Wireless Wide Area Networks)

Bir ülke ya da dünya çapında yüzlerce veya binlerce kilometre mesafeler arasında iletişimi sağlayan ağlara Geniş Alan Ağları (WAN-Wide Area Networks) 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. Uzak yerleşim birimleriyle iletişimin kurulduğu bu ağlarda çok sayıda bilgisayar çalışabilir. WWAN uygulamalarına örnek olarak GSM, GPRS ve 3G sistemleri sayılabilir. WWAN'larda trafik yükünün büyük kısmı ses iletişimi ile ilgilidir. Ancak son yıllarda yoğun olarak veri iletişimi ve internet erişimi talepleri yaşanmaktadır.

1.3.5.1 IEEE 802.20 Standardı

IEEE 802.20 standardını geliştiren çalışma grubu gerçek yüksek hızlı mobil broadband sistemleri üzerinde odaklanmıştır. 802.16 teknolojisinin sunduğu sabit genişbant uygulamalarını mobil imkanlarla sunmak amacıyla, IEEE, Mobil Genişbant Kablosuz Erişim Çalışma Grubu (MBWA-Mobile Broadband Wireless Access Working Group) adındaki grubu ile IEEE 802.20 standartlarını oluşturmaya çalışmaktadır. 3.5 GHz frekans altında çalışan bu teknoloji üzerinde, IP veri iletimi desteği en iyileştirilmeye çalışılmaktadır[IEEE MBWA,2005].

1.3.5.2 GSM (Global System For Mobile Communication)

GSM bugün dünyada en çok kullanılan mobil telefon ve taban istasyonları üzerinden aktarma yöntemiyle uzun mesafeler arasında cep telefonu ile ses ve veri haberleşmesini sağlayan sistemlerdir.

GSM sistemi, 1982 senesinde CEPT(European Conference of Postal and Telecommunications) tarafından hayata geçirilmiştir. Bu konferanstan sonra 1989 senesinde ETSI (European Telecommunications Standards Institute) kurulmuştur. 1992 senesinde ilk GSM şebekesi çalışmaya başlanmıştır. GSM' de ses küçük veri blokları halinde 900-, 1800- veya 1900 MHz frekans bandından iletilmektedir. Verici tarafından tüm frekanslar küçük zaman dilimlerine bölündüğü için aynı zamanda tek frekanstan birden çok, ama en fazla 8 görüşme yapılabilmektedir. Bu çalışma sisteminin ismi TDMA(Time Division Multiple Access)'dır[Gsm World,2011].

1.3.5.3 3G

3G mobil haberleşme teknolojisi, 1G ve 2G sistemlerin sağladığı sesli iletişim teknolojisine ek olarak esas itibariyle veri iletimine odaklanmaktadır. 1G ve 2G teknolojilerinden farklı olarak 3G mobil şebekeler kullanıcılara çoklu ortam hizmetleri sunmak için tasarlanmıştır ve sesin yanında görüntü, veri ve yüksek hızda internet bağlantısı sağlanabilmektedir. 3G sistemler çok hareketli kullanıcılara 144 kbps, yavaş ve orta hızlı kullanıcılara 384 kbps ve durağan kullanıcılara ise 2 Mbps hızında veri hızı sağlamaktadır. Günümüzde iki 3G teknolojisi olan UMTS ve CDMA 2000 diğer standartlar arasında öne çıkmaktadır [Holma H.,Toskala A.,2000].

3G teknolojilerinin ilki UMTS, GSM sistemlerinin yeni neslidir, ancak radyo erişim (Radio Access) tekniği olarak Geniş bant Kod Bölmeli Çoklu Erişim (Wideband

Code Division Multiple Access-WCDMA) kullanmaktadır. Mobil iletişim altyapısı olarak GSM sistemini kullanan servis sağlayıcılar için 3G hizmetlerini sunmak için tercih edecekleri en muhtemel teknolojinin WCDMA olacağı düşünülmektedir.

3G teknolojilerinin ikincisi WCDMA'ya rakip olarak gösterilen ve CDMA2000 olarak adlandırılan Çok taşıyıcılı CDMA (MC-CDMA) teknolojisidir. CDMA2000, CDMA teknolojisine dayalı 2G şebekeler için 3G hizmetlere en uygun geçiş yoludur.

Gelecekte 3G nesil ağların yerini alacak olan internet protokol (Internet Protocol-IP) temelli 4G nesil ağlar, kullanıcılara yüksek kapasite, bit başına düşük maliyet ve yüksek hızda erişim imkânı sunmayı planlamaktadır. Amacı günümüzde var olan hücresel sistemler yerine dünya çapında IP tabanlı tek bir hücresel ağ oluşturmaktır. 4G nesil sistemler tamamıyla paket anahtarlamalı sistemler olup tüm devre elemanları dijitaldir. Çoklu ortam uygulamaları örneğin canlı olarak video seyretme gibi uygulamalar büyük bir bant genişliğine ihtiyaç duyar. Ağ güvenliği çok önemlidir. 4G nesil sistemler için potansiyel teknolojiler; UWB, OFDM ve Çok Giriş-Çok Çıkış (Multi Input -Multi Output-MIMO) anten sistemleridir [Dubuc C., Starks D., Creasy T., 2004].

1.3.5.4 GPRS (General Packet Radio Service)

GPRS, GSM ve TDMA ağları için geliştirilmiş olan paket temelli veri taşıyıcı bir servistir. GPRS yüksek hızlarda (115 kilobit/s) kablosuz internet ve diğer veri iletişimine olanak sağlar. GPRS teknolojisi, kullanıcıya yüksek hızlı bir erişimin yanı sıra, bağlantı süresine göre değil gerçekleştirilen veri alışveriş miktarına göre ücretlendirilen ucuz iletişim olanağı da sağlar. Bu yönüyle GPRS, "sürekli bağlantı halinde" olma imkânının gerçekleşmesi yolunda atılmış çok önemli bir adımdır

GPRS platformu sayesinde telefonunuzun özelliklerine göre cep telefonunuzdan ya da dizüstü bilgisayar ve cep telefonu aracılığı ile profesyonel kullanıcıların İnternet'e ve işyerlerindeki kurumsal bilgisayar ağlarına (intranet) bağlanmaları da mümkün olmaktadır. Dizüstü bilgisayarları ile İnternet'e kablosuz erişim sağlamak isteyen kullanıcılar, cep telefonlarını İnternet'e bağlanmak için gerekli modem olarak kullanarak Superonline GPRS ile kesintisiz İnternet erişimi sağlarlar.

GPRS, mobil iletişim teknolojisinde halen kullanılmakta olan devre anahtarlama (sadece tek bir kullanıcıya tahsis edilen bir hat üzerinden sürekli bağlantı) metodu yerine paket anahtarlama (aynı hattın birden çok kullanıcı tarafından paylaşıldığı ve iletişim hızının 115 Kb'ye kadar çıktığı bir yapı) yöntemini kullanmaktadır[GPRS,2011].

1.4 IEEE 802.11 Kablosuz Yerel Alan Ağ Standartları

IEEE 802.11 standart takımı kablosuz yerel ağlar içindir. IEEE LAN/MAN standart komitesi tarafından 5 GHZ ve 2.4 GHZ halk bandı (public spectrum band) içinde geliştirilmiştir. Bina içi veya yerleşke alanında, gezici kullanıcılar için geliştirilmiş bir teknolojidir. 802.11 terimlerine rağmen, Wi-Fi sıklıkla kullanılan ve en çabuk ticarileşen bir isim olmuştur. Wi-Fi, Wireless Fidelity kelimelerinin ilk iki harfinin kullanılarak ortaya çıkartılmış bir kısaltmadır. 802.11b standardı Wi-Fi olarak adlandırılmış olup, kısaca kablosuz ağ olarak ta kabul edilebilinir. 802.11 ailesi over-the-air modülasyon tekniğini içerir ki bu da aynı basit protokolü kullanır. En popüler olan kablosuz ağ standartları 802.11b ve 802.11g olarak tanımlanmıştır. 802.11a ilk kablosuz ağ standardı olmasına rağmen 802.11b geniş kitleler tarafından kabul edilmiştir[Kablosuz Ağ Standartları,2003]. Bu gelişmeleri sırayla 802.11g ve günümüzde Türkiye'de de kullanımı yaygınlaşmaya başlayan 802.11n standartları takip etmiştir.

1.4.1 IEEE 802.11 legacy

IEEE 802. 11 standart takımı kablosuz yerel ağlar yani WLAN bilgisayar iletişimi içindir. IEEE LAN/MAN standart komitesi tarafından 5 GHZ ve 2.4 GHZ halk bandı içinde geliştirilmiştir. 802.11 ailesi havadan iletişim (over-the-air modulasyon) tekniğini içerir ki; bu da aynı basit protokolü kullanır. En popüler olanları 802.11b ve 802.11g protokolü olarak tanımlanmış ve orijinal standartlara eklenmiştir. 802.11a ilk kablosuz ağ standardı olmasına rağmen 802.11b ilk geniş kitleler tarafından kabul edilen standartdır. Bunu sırayla 802.11g ve yeniliklerini işleyeceğimiz 802.11n takip etmiştir[Scarfone K., Dicoi D., Sexton M.,2008].

1.4.2 IEEE 802.11a

1999 yılında standart olan 802.11a, 5 GHz frekansta ve maksimum 54 Mbps (Mbps/sn) hızında çalışabilir. Ancak bazı faktörler bant genişliğinin önemli bir kısmını tüketmektedir. Yonga üreticilerine göre 802.11a protokolünün ulaşabileceği en yüksek veri transfer hızı 22–26 Mbps arasında bir değerdir. Modülasyon tekniği olarak OFDM (Orthogonal Frequency Division Multiplexing - Dikey Frekans Bölüşümlü Çoğullama) kullanır.[Chang R.,1996,Bahai A.,Saltzberg B.,Ergen M.,2004]

Yüksek frekans olmasına karşı 802.11b'ye göre uzak mesafelerde setlerden ya da engellerden geçemezler. Sebebi Frekans arttıkça dalga boyu küçüldüğü için karşılaştığı engellere daha çok takılır. Bunun için çok odalı ya da engelin çok olduğu ortamlarda verimsizdir. 802.11b ve 802.11g standartlarıyla uyumsuzdur. Kapsama alanı kapalı alanlarda 7,5–22,5 metredir. Açık alanlarda 30–45 metredir.

802.11a'da 802.11b gibi değişik hız seviyelerinde çalışabilmektedir. 802.11b 11, 5. 5, 2 ve 1 Mbps veri transfer hızlarına destek verirken, 802.11a 48, 36, 24, 18, 12, 9 ve 6 Mbps veri transfer hızına destek vermektedir.

802.11a'da 5 GHz spektrumunun Amerika Birleşik Devletleri'nde kullanılan iki alt bandında (5.15-5.25 ve 5.25-5.35 GHz) eşzamanlı operasyon için 8 kanal mevcuttur. Her biri 20 Mhz genişliğinde olan ve 52 adet taşıyıcı sinyal destekleyebilen bu 8 kanalın merkez noktaları 5.18, 5. 2, 5.22, 5.24, 5.26, 5.28, 5.30 ve 5.32'dir. Var olan kanallardan bağımsız olarak 802.11a herhangi tek bir kanalı herhangi bir zamanda kullanabilir. Eğer birden fazla erişim noktanız varsa çok daha fazla sayıda eşzamanlı kullanıcıyı destekleyebilirsiniz[IEEE, 2007, CISN,2002].

1.4.3 IEEE 802.11b

Eylül 1999 yılında standart olan 802.11b, 2.4 GHz frekansta maksimum olarak 11 Mbps bant genişliğinde çalışmaktadır. Fakat ortalama değer olarak 4.3 Mbps hızda çalışır. Ticarileşmiş ilk standarttır. Modülasyon tekniği olarak DSSS (Direct Sequence Spread Spectrum) kullanır[Kaplan Y.,2002]. Bu spektrum aynı zamanda kablosuz telefon ve çoğu bluetooth ürünleri tarafından da kullanılmaktadır. Kapsama alanı kapalı alanlarda 30–45 metredir. Wi-Fi uyumlu farklı marka cihazlar, birbirleriyle uyumlu çalışabilir. Ancak 802.11b standardında da bazı sorunlar vardır. Öncelikle video, grafik, ses ağırlıklı hale gelen veri ortamını desteklemekten uzaktır ve bant genişliği ve gerçek zamanlı veri iletimine olanak sağlayacak servis kalitesi ve önceliklendirme desteği bulunmamaktadır. Ayrıca diğer donanımların yarattığı radyo paraziti bu standardın kullandığı frekansı önemli ölçüde etkilemektedir. Bu donanımların bazıları; 2.4 GHz frekansında 1 Mbps maksimum veri transfer hızında çalışan WPAN uygulamalarında kullanılan Bluetooth donanımlar; mikro dalga fırınlar ve telsiz telefonlardır.

Diğer bir problem ise 802.11b'de 2.4 Ghz'den 2.4835 Ghz frekans bandında eşzamanlı operasyon için 3 kanal kullanılabilmesidir. Bu aralıkta belirlenen 11 merkez frekans vardır. 2.412, 2.417, 2.422, 2.427. 2.432, 2.437, 2.442, 2.447, 2.452 ve 2.462 ancak aktif kanallar arasında 25 Mhz boşluk gerekli olduğu için genellikle 3 kanal eşzamanlı olarak kullanılabilmektedir. Daha fazla kanal kullanıldığı zaman parazit ve gürültü olasılığı yüksektir[IEEE,2007].

1.4.4 IEEE 802.11c

Bu standardın görevi, Kablosuz Erişim Noktaları (AP-Access Point)'lar arasında köprüleme işlemlerini yapmaktır. Diğer 802.11 standartlarının MAC (Media Access Control) alt katmanında çalışır. Şirketler ve üniversiteler bu standardı, ağlarını genişletmek için sıklıkla kullanırlar [Barnes C.,Bautts T.,Lloyd D.,2002 ,Ritz J.,2003].

1.4.5 IEEE 802.11e

IEEE 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[Barnes C.,Bautts T.,Lloyd D.,2002].

1.4.6 IEEE 802.11f

IEEE 802.11f standardı, kontrollerin taban istasyonları arasındaki birlikte çalışabilirliği sağlayan farklı üreticilerin erişim noktaları arasında dolaşımını olanaklı kılmak için çalışmaktadır. Böylelikle kullanıcılar ağ içindeki farklı AP'leri kullanabilmektedir[IEEE,2003].

1.4.7 IEEE 802.11g

2003 yılında standart olan 802.11g, 2.4 GHz frekansta teorik olarak maksimum 54 Mbps hızında çalışabilir, ama 802.11g standardının ulaşabileceği en yüksek veri transfer hızı 19 Mbps'dir. Modülasyon tekniği olarak oda 802.11a gibi OFDM'yi kullanır. 802.11b ürünleriyle uyumludur. Günümüzde (2011'de) kullanılan kablosuz ağ ürünleri ister dizüsütü bilgisayar ister erişim noktası olsun 802.11g uyumludur. Kapsama alanı kapalı alanlarda 30–45 metredir. 802.11b ile aynı frekans spektrumunu kullandığından standartlaş-ması kolay olmuştur. Frekansın 2.4 GHz olması ve bu frekansta 802.11g'nin 802.11b'ye göre daha yüksek hızlarda veri iletişimi sağlaması tercih sebebedir. Aynı zamanda modülasyon tekniği olarakta 2.4 GHz'in çakışmalara daha toleranslı olması 802.11g'nin günümüzde kullanılmasını sağlamaktadır [IEEE,2003]. Fakat 2007 yılında bu standarda göre daha yüksek hızlara çıkabilen ve daha geniş kapsama alanına sahip olan 802.11n geliştirilmiştir.

1.4.8 IEEE 802.11i

Bu standart güvenlikli odaklıdır. 802.11 standartları için güvenlik ve kimlik denetleme mekanizmaları geliştirir. MAC katmanında çalışır. Tezde kablosuz ağlarda güvenlik politikaları isimli bölümde detaylı olarak anlatılacak olan bu standart, kablosuz ağlar için başlangıçta geliştirilen şifreleme standardını, algoritmasını vs tamamen değiştirmektedir[IEEE,2004].

1.4.9 IEEE 802.11n

IEEE 802.11n, 2.4 GHz ve 5 GHz frekanslarında 248–300 Mbps arasında yüksek hız sağlamaktadır. Fazlasıyla arttırılmış veri aktarım hızı ve kapsama alan genişliği 802.11n'in en önemli özellikleridir. IEEE tarafından bu standardın ilk taslağı Temmuz 2008'e yetiştirilmeye çalışılmaktadır. Mart 2009'da da tam anlamıyla standart olması hedeflenmektedir. Ancak başka bir organizasyon olan Wi-fi Alliance (Wireless Fidelity Alliance- Kablosuz network birliği) tarafından 802.11n taslak 2.0 günümüzde yayınlaşmış ve bu kuruluş tarafından cihaz üreticilerine lisans verilmeye başlanılmıştır. Belge, IEEE 802.11n standardının erken bir taslağını kullanır. 802.11n taslak 2.0, 802.11n cihazları için istenilen asgari koşulları belirler. Bu standart MIMO (Multiple Input Multiple Output-Çoklu Giriş Çoklu çıkış) teknolojisini kullanır. MIMO ile daha açıklayıcı bilgi ileriki bölümlerde verilecektir.

1.4.10 IEEE 802.11y

IEEE 802.11y standardı Haziran 2008'de yayınlanmıştır. 54 Mps hızında veri iletişimi yapar. Diğer stardandartlar 2. 4 GHz de çalışırken bu standard 3.7 GHz'de çalışmaktadır. Çıkış gücü yükseltilmiştir. Bunun ona kazandırdığı bina içi 50 m ve bina dışı 5 km'ye kadar kapsama alanıdır[802.11y Standardı,2008].

Standart	Frekans Bandı	Veri Hızı	Mesafe (Bina İçi)	Mesafe (Bina Dışı)
802.11	2.4GHz	1-2 Mbps	30 M	150 M
802.11a	5 GHz	54 Mbps	30 M	100 M
802.11b	2.4GHz	11 Mbps	30 M	150M
802.11g	2.4GHz	54 Mbps	30 M	150 M
802.11h	5 GHz	54 Mbps	30 M	100 M
802.11n	2.4GHz - 5 GHz	248 Mbps	70 M	250 M
802.11y	3.7 GHz	54Mbps	500 M	5000 M

Tablo 1. 7 802.11 Kablosuz LAN Standartlarının Karşılaştırılması.

[IEEE 802.11: Wireless Local Area Networks, 2011]

1.5 Kablosuz Ağlarda Modülasyon Teknikleri ve Yapıları

WLAN sistemleri lisans ve kullanım ücreti gerektirmeyen ISM frekans bantlarında çalışmaktadır. Bu bantlar aynı zamanda telsiz servislerinin kullanımı için tahsisli olduğundan WLAN sistemleri enterferansa(frekans dalgalarının kesişmesi)

dayanıklı teknolojiler üzerine kurulmak zorundadır. Bunun için WLAN sistemlerinde her bir standardın modülasyon tekniği, diğer kablosuz iletişim teknolojileri ile parazit yaratmaması için frekans spektrumunu verimli kullanan ve enterferanstan az etkilenen teknolojiler geliştirilmiştir. Bunlara örnek olarak FHSS, DHSS ve 802.11n teknolojisi MIMO verilebilir[Öztürk E., 2004, Kaplan Y.,2002].

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

Radyo frekans sinyalinin geniş bir bant aralığına oturtulması ve bu aralığa yayılmış olan sinyalin verici-alıcı cihazlar tarafından işlenmesi teknolojisidir. Yayılı spektrum üzerinde doğrudan diziyle yayma (direct sequence) modülasyonu kullanmaktadır. Cihazlar 2.4 – 2.5 Ghz frekansını kullanmaktadır. 802.11b standardı DSSS teknolojisini kullanmaktadır. DSSS fazla bant genişliğine, daha yüksek veri iletişim hızına sahiptir ve enterferanstan daha az etkilenmektedir.[Öztürk E.,2004, Kaplan Y.,2002]

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

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

seviyeli bir güvenlik sağlar. FHSS tekniği için 2402–2480 MHz frekans aralığında 1 frekansta 79 kanal bulunmaktadır. Bu sayı 75'den az olmamak kaydıyla ülkeden ülkeye değişim göstermektedir. 802.11d'de tanımlanmasına rağmen 802.11 grubu ve cihaz üreticileri tarafından pek rehabet görmeyen bir modülasyon yöntemidir. Daha ucuz olmaları ve daha düşük güç tüketmelerine rağmen düşük iletim oranı ve iletim mesafesinde işletilebilirler. 2Mbps veri iletimi sağlarlar[Öztürk E.,2004, Kaplan Y.,2002].

1.5.3 Dikey Frekans Bölüşümlü Çoğullama (OFDM-Orthogonal Frequency Division multiplexing)

OFDM radyo dalgaları üzerinden büyük miktarda veri transferi yapmak için kullanılan bir frekans bölüşümlü çoğullama modülasyon tekniğidir. OFDM radyo sinyalini daha küçük alt sinyallere bölüp aynı anda farklı frekanslardan alıcıya gönderme yöntemi ile çalışır. OFDM bir taşıyıcı yerine çok sayıda taşıyıcı kullanılan bir modülasyon tekniği olarak da bilinir. Bu teknikte sinyaller fiziksel engellerle karşılaştığında dağılmayıp, engelin çevresinden dolaşmaktadır. OFDM sinyal iletiminde meydana gelen çapraz karışmayı azaltan ve çoklu-yol gecikme yayılmasına ve kanal gürültüsüne tolerans tanıyan bir yöntemdir. Bu yüzden pek çok kablosuz uygulama için oldukça uygundur[Öztürk E.,2004 ,Wireless Communication,1995].

1.5.4 Taşıyıcı Algılaması Çoklu Erişim/Çakışma Kaçınma (Csma/Ca-Carrier Sense Multiple Access/Collision Avoidance)

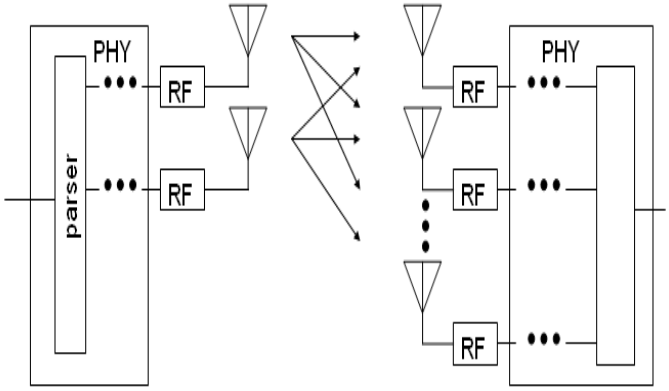
Ağdaki çarpışmaların önüne geçebilmek için kullanılan ağ bağlantı protokolüdür. Kablosuz ağ trafiğini sağlar. CSMA/CA gerçek veri dağıtımı yapılmadan önce çarpışmaları dinlemek için ağa bir sinyal gönderir, çarpışma duyduğunda, WLAN Üzerindeki diğer aygıtlara hiçbir veri yayınlamamalarını söyler. IEEE 802. 11 iletim şekli ve iletim ortamını tanımladığı için OSI'nin birinci ve ikinci katmanında faaliyet göstermektedir. Modülasyon şekilleri olan DSSS, FHSS, OFDM OSI'nin fiziksel katmanı ile ilgilidir. Diğer güvenlik ve iletim ile ilgili kısımlar ikinci katmanda (veri bağı) işlenir[Öztürk E.,2004].

1.5.5 Çoklu Giriş Çoklu Çıkış (MIMO-Multiple Input Multiple Output)

802.11n, MIMO adı verilen bir protokol sayesinde 2.4 GHz ve 5 GHz frekanslarının her ikisini de aynı anda kullanabilmektedir. MIMO teknolojisi, iletilecek bir bilginin parçalara ayrılıp farklı antenler üzerinden karşı tarafa gönderilmesini sağlar. Diğer standartlarla çalışan cihazlar bir anten üzerinden bir yayın yaparken, 802.11n teknolojisine sahip ağ cihazları gönderi tarafında veya daha fazla yayın yaparken, alım tarafında birden fazla anten kullanırlar ve birden fazla alınan/gönderilen yayınları birleştirirler. Gönderilen veriler farklı rotalar takip ederek (örnek: duvarlardan, kapılardan ve diğer eşyalardan yansıyarak) alıcı antene farklı zamanlarda ve birden fazla kere varır. MIMO teknolojisi bu durumu kendi lehine kullanarak işaretin güçlenmesini ve daha uzaklara iletilmesini sağlar. [CISN,2002] MIMO teknolojisinin yapısı ileriki bölümlerde açıklanmıştır

1.5.5.1 MIMO Temelleri

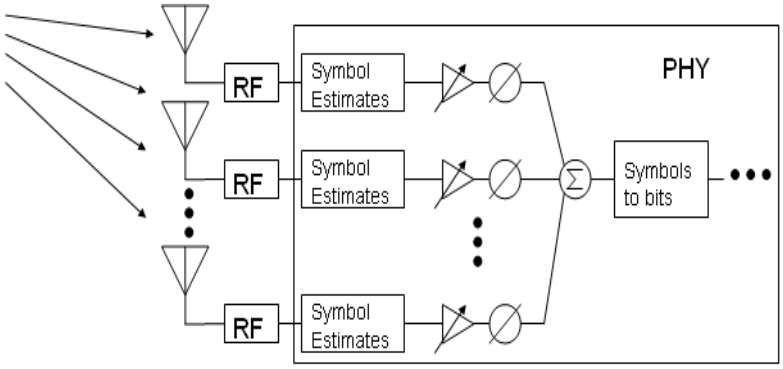
- İstemci ve Erişim noktasının her ikisinde de benzer MRC (Maximum Ratio Combining) tabanlı donanıma ihtiyaç duyulur.
- Aynı frekans üzerinden aynı anda çoklu veri akımı sağlanabilir. Bu da yüksek ortalama veri transferine olanak sağlar.
- Hem veri oranını arttırmak için hem de bağlantının gücünü arttırmak için kullanılabilir.
- 802.11 a/b/g ile uyumlu değildir.



Şekil 1. 5. MIMO'da Alıcı – Verici Yapısı

1.5.5.2 Maximum Ratio Combining (MRC)

MRC Temel bantta DSP (Digital Signal Processor) teknikleri kullanılarak yapılır. Çoklu antenler ve çoklu tam radyo frekansları paralel kullanılır. Gönderilen sinyalin kopyaları temel bantta maksimum SNR (signal to noise ratio) için doğrulanır ve birleştirilir[Yoshio K.,Tetsuki T.,2002].

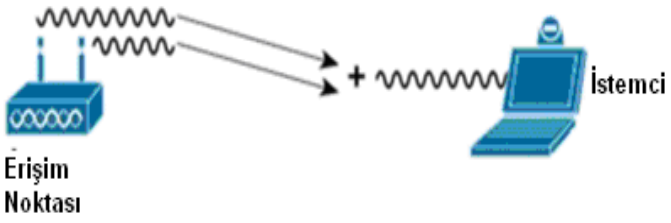


Şekil 1. 6. MRC Yapısı

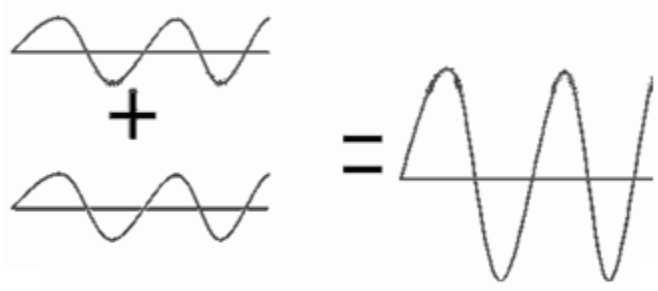
1.5.5.3 Sinyal Oluşturma (Beamforming)

MIMO teknolojisi, alıcıda SNR'ı iyileştirmek için kullanılan diğer tekniklerin avantajlarını kullanılır. Bunlardan biriside Transmit Beamforming'tir (gönderim sinyali oluşturma). Beamforming işlemi ilk sürüm tarafından desteklenmemektedir[Yoshio K., Tetsuki T.,2002].

Bu teknikte, erişim noktasındaki antenler tarafından gönderilen sinyaller, alıcı tarafından ayrı ayrı alınıp, kendi içerisinde sinyaller birleştirilerek, sinyal gücü arttırılır. Bu işlem Constructive Interference (Yapıcı karışma) olarak adlandırılır. Transmit Beaforming işlemi aşağıdaki şekilde gösterilmektedir.

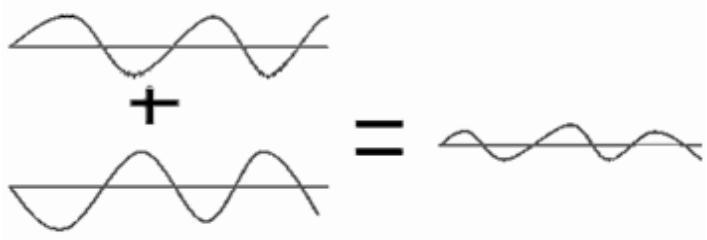


Şekil 1. 7. İletken Sinyal oluşturma (Transmit Beamforming) [Gezgin D.,Buluş E.,Buluş N.,2008]



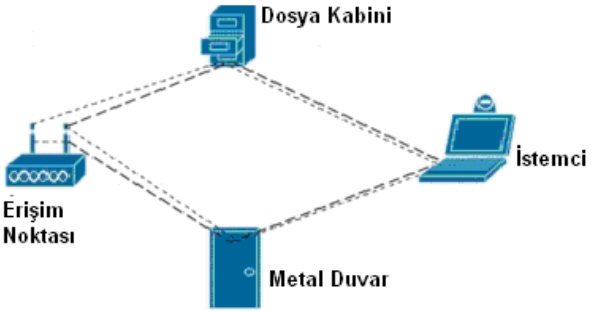
Şekil 1. 8. Yapıcı Karışma (Constructive Interference) [Gezgin D.,Buluş E.,Buluş N.,2008]

Fakat beamforming işlemi, eski standart aygıtlarda iki sinyal arasındaki gecikmeden ötürü parazitlere ve veri kayıplarına sebep olabilir. Bu da Destructive Interference (Yıkıcı karışma) olarak adlandırılır. [Gezgin D.,Buluş E.,Buluş N.,2008]



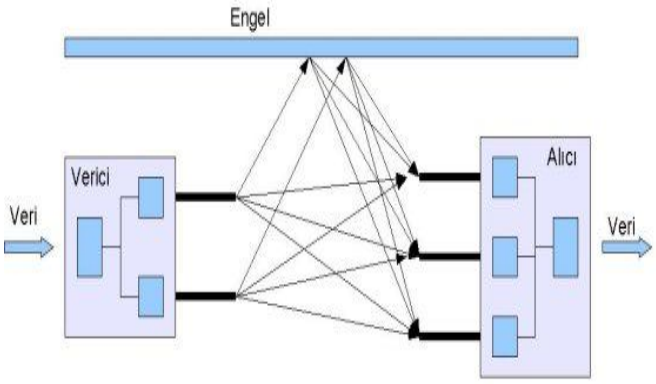
Şekil 1. 9. Yıkıcı Karışma (Destructive Interference) [Gezgin D.,Buluş E.,Buluş N.,2008]

Genel anlamıyla MIMO, birden fazla antenle iletim tekniğinde geçmektedir. Çok-yollu Yayılım (Multipath Propogation) gibi olguların kullanımıyla, bant genişliğinin verimini artıran bir teknoloji denilebilir. Radyo dalgaları, yayılımları sırasında engellere çarpıp yansımakta veya sönümlenmektedir. Geleneksel anten teknolojisinde, bu yansımalar sıkıntılar yaratabilmektedir. Örneğin Televizyon izlerken izlediğiniz kanalın görüntüsünün bir kopyası, biraz kaymış gibi ekranda görünmesi gibi.



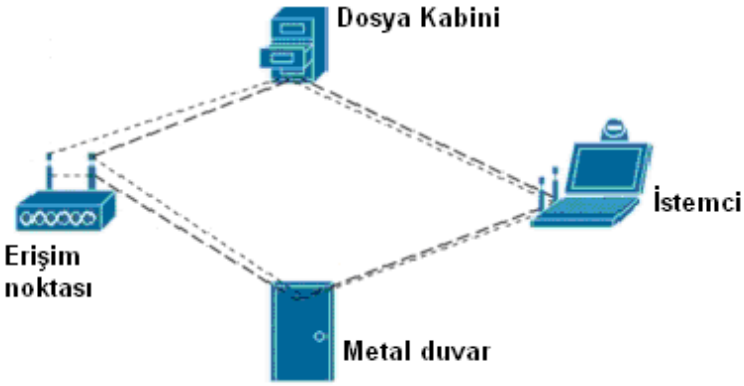
Şekil 1.10 Çoklu Yol (Multipath) [Gezgin D.,Buluş E.,Buluş N.,2008]

MIMO, bu etkiyi, aynı frekans bandında, birim zamanda iletilebilecek veri miktarını artırmak için kullanır. Birden fazla anten kullanımıyla, veri parçalar halinde gönderilir ve karşı tarafta da yine fazla sayıda anten tarafından algılanır. Her bir anten tarafından alınan veri, bir Sayısal İşaret İşleyici (DSP - Digital Signal Processor) kullanılarak birleştirilir. Gözünüzde canlanması için, yine ayrıntıdan uzak, temel düzeyde bir çizim yardım edebilir.



Şekil 1.11 Çok-yollu Yayılım[Gezgin D.,Buluş E.,Buluş N.,2008]

Şekilde, vericiye gelen veri, içeride parçalara ayrılıp, radyo dalgaları halinde dışarıya aktarılır. Antenlerden yayılan dalga, hem doğrudan doğruya, hem de ortamdaki engellerden yansıyarak alıcıya ulaşır. Alıcı, üç anteninde algıladığı veriyi, sayısal işaret işleme yardımıyla birleştirerek, esas veriyi tekrar oluşturur.



Şekil 1.12 Uzaysal Çoklama (Spatial Multiplexing)[Gezgin D.,Buluş E.,Buluş N.,2008]

Ek olarak, MIMO teknolojisinde kullanılan anten sayısına ya da full duplex (çift yönlü) iletişime göre veri aktarım hızı farklı değerlerde olabilir. Aşağıdaki şekil standartların ortalama özelliklerini göz önüne koymaktadır. Yeni bir standartlaşmaya gidildiği için birçok sorunda karşımıza çıkabilir. Bunlar eski kablosuz cihazlarla uyum, maliyet, güvenlik konularıdır. Kablosuz ortamlarda yüksek hız, kablolu ağı daha ciddi bir şekilde tehdit edip, tüm sektörlerde yüksek iş kapasitesi demektir[802.11n Standardı,2011].

1.6 Kablosuz Yerel Alan Ağlarda Çalışma Modları ve Ağlar

IEEE 802.11 kablosuz yerel alan ağlarında iki farklı çalışma modu bulunmaktadır. Bunlar Tasarsız mod ve Tasarlı Mod'dur.

1.6.1 Tasarsız Mod (Ad Hoc Mode)

Kablosuz istemciler herhangi bir Erişim Noktasına bağlanmaksızın direk birbirleriyle bağlantı kurmaktadırlar (Peer-to-Peer bağlantı). Bu tür ağlar aynı zamanda Bağımsız Temel Hizmet Takımı (IBSS-Independent Basic Service Set) olarak isimlendirilmektedirler.



Şekil 1.13 Tasarsız (Ad Hoc) Mod Yapısı [UGL2454-VPA,2005]

1.6.1.1 Mobil Tasarsız Modlu Kablosuz Ağları

Vanet olarak isimlendirilen bu tip ad hoc ağlar hareket halindeki araçlardan oluşturulan ad hoc ağlardır. Çoğunlukla askeri amaçla kullanılan ağ tipidir.

1.6.1.2 Kablosuz Duyarga Ağları (WSN-Wireless Sensor Networks)

Nem, sıcaklık, basınç, ses, ışık, hareket, sismik algılayıcı gibi birçok farklı tipte duyargalardan veri toplamak amacı ile oluşturulan ad hoc kablosuz ağ sistemleridir. Çok sayıda cihazdan oluşan ve değişkenlik gösterebilecek ağlardır. Pil üzerinden beslendikleri için minimum sistem kaynağı ile haberleşmesi istenen ağlardır. Çoğu zaman pilleri tükenince kullanım ömürlerini doldururlar. Uygulama alanları; askeri sistemler, endüstriyel otomasyon, bina otomasyonu, jeolojik ölçümlerin takibi, biomedikal ağlardır.

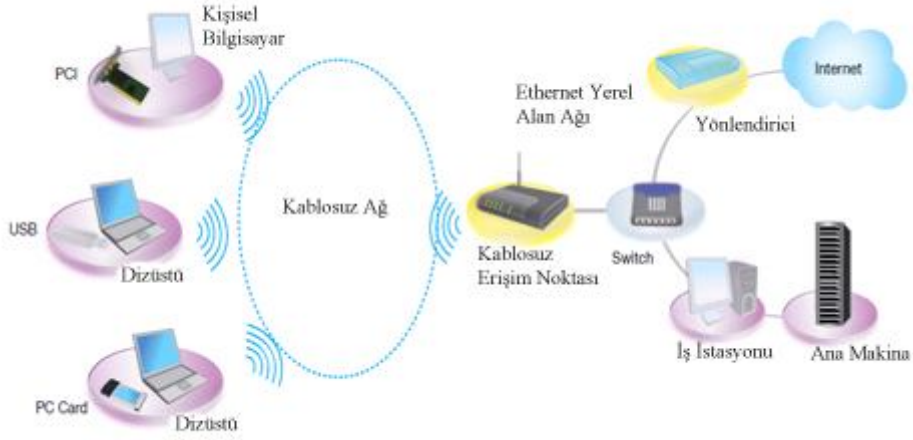
1.6.1.3 Kablosuz Örgü Ağları (Wireless Mesh Networks)

Geniş bölgelerde veri erişiminin kablo altyapısında bağımsız olarak sağlanması için oluşturulan kablosuz ad hoc ağlardır. Henüz taslak IEEE 802.11s ile bu tipteki ağlara standart getirilecektir. Alt yapıları çoğu zaman sabit veya kısıtlı hareket eden kablosuz erişim yapabilen cihazlardan oluşurlar. Kullanılan cihazlar, sadece kablosuz erişim noktaları, istemciler ya da ikisi birden kullanılan hibrit sistemlerdir. Sabit noktalardan oluştukları için pil sıkıntıları pek yoktur. Ses, Görüntü veya veri haberleşme için kullanıldıkları için gecikme ve band genişliği önemli ölçütlerdir.

1.6.2 Tasarlı Mod (Infrastructure Mode)

Kablosuz istemciler bir veya birden çok Erişim Noktasına bağlanmakta ve tüm veri trafiği bu Erişim Noktaları üzerinden akmaktadır. İstemci direk karşı taraf ile konuştuğunu zanneder fakat bütün trafik AP üzerinden geçer. Tek Erişim Noktası bulunan ağlar Temel Servis Seti (BSS-Basic Service Set), çoklu Erişim Noktası bulunan

ağlar ise Genişletişmiş Servis Seti (ESS-Extended Service Set) olarak isimlendirilmektedirler.



Şekil 1.14 Tasarlı (Infrastructure) Mod Yapısı [UGL2454-VPA,2005]

1.7 Kablosuz Yerel Alan Ağ Topolojileri

Topoloji kavramı, elemanların fiziksel ve ya mantıksal dizilişleri anlamına yani ağa bağlanan düğüm noktalarının (bilgisayarlar, ağ yazıcıları, sunucular, vs.) yerleşimini simgelemektedir. Günümüzde (2011'de) kablosuz iletişim ağlarında üç ana topoloji tipi kullanılmaktadır: Bunlar Yıldız (Star), Noktadan Noktaya (PtP) ve Örgü (Mesh) topolojileridir.

1.7.1 Yıldız Topolojisi (Star Topology)

Yıldız topolojisi (ki günümüzde en fazla kullanılan topoloji tipi budur) söz konusu olduğunda bir ağdaki iletişimi düzenlemek için bir taban istasyonu veya erişim noktası kullanılmaktadır. Bir noktadan diğerine giden bilgi önce göndericiden erişim

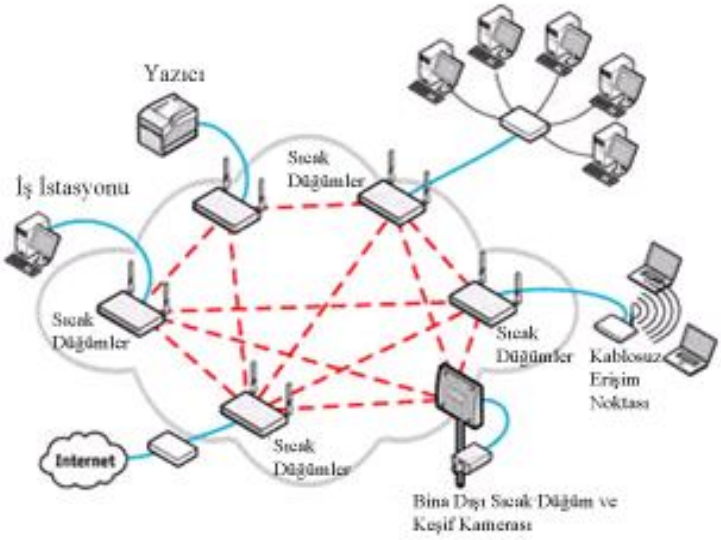
noktasına geliyor, oradan da hedef noktaya aktarılmaktadır. Bu erişim noktası ya da istasyon ayrıca kablolu bir ağa köprü görevi de görebilir. Böylece kablosuz olarak bağlanan istemciye ağ üzerindeki diğer bilgisayarlara, internete veya diğer ağ aygıtlarına erişim sağlanabilmektedir.

1.7.2 Örgü Topolojisi (Mesh Topology)

Ağ örgüsü topolojisi ise yıldız topolojisinden biraz daha farklıdır. Sistem aynı olmasına rağmen ortamda bir erişim noktası bulunmamaktadır. Birbirinin kapsama alanındaki her aygıt birbiri ile haberleşebilir. Daha gelişmiş sistemlerde AP'ler ya da HotPointler düğüm olarak görev yapar. Şekil 1.15'de bir örgü ağ yapısı görülmektedir.

1.8 Kablosuz Ortam Ağ Bileşenleri

IEEE 802. 11 Kablosuz yerel alan ağlarında kullanım alanlarına göre biden çok aygıt bulunmaktadır. Kablosuz yerel alan ağlarında bulunan temel bileşenler aşağıda sıralanmaktadır.



Şekil 1.15. Örgü (Mesh) Topolojisi

1.8.1 Kablosuz İstemci (Wireless Client)

En az bir adet 802.11a/b/g kablosuz ağ adaptörüne sahip olan kişisel bilgisayarlar, dizüstü bilgisayarlar, el bilgisayarları, cep telefonları istemci olarak kabul edilir.

1.8.2 Kablosuz Erişim Noktası (WAP - Wireless Access Point)

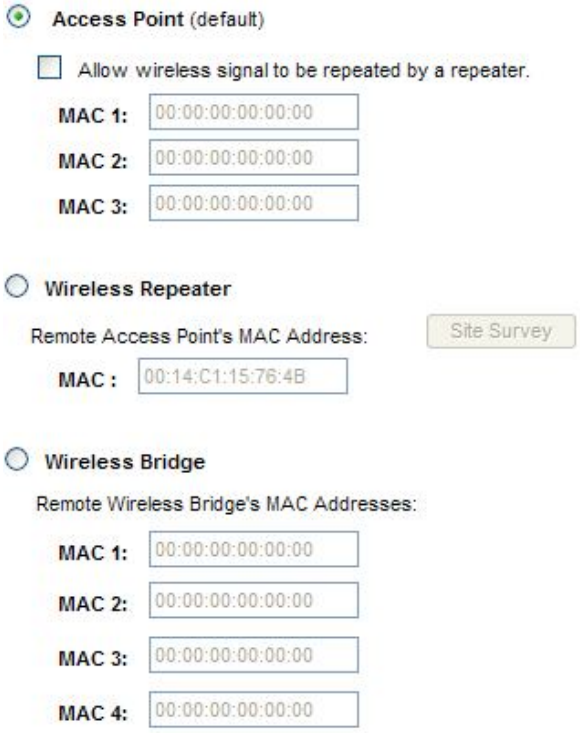
Erişim noktası kısaca AP ya da WAP adıyla bilinir. Erişim noktası, kablolu bir Ethernet ağına kablosuz erişim sağlar. Erişim noktası, hub'a, anahtara veya kablolu yönlendiriciye takılır ve kablosuz iletişim sinyalleri gönderir. Bu, bilgisayarların ve

aygıtların kablolu ağa kablosuz olarak bağlanmasını sağlar. Erişim noktaları hücresel telefon kuleleri gibi davranır: bir konumdan diğerine geçebilir ve ağa kablosuz erişiminiz devam edebilir. Kablolu ağlardaki Hub isimli cihaza karşılık gösterilebilinir. Gelen paketi havaya gönderirler ve tüm istemciler ilgili pakete ulaşabilir. Erişim noktaları SSID (Service Set ID)'leri ile ayırt edilirler. Erişim Noktaları periyodik olarak beacon paketlerini havaya göndermek suretiyle varlıklarını (SSID bilgilerini) mevcut istemcilere bildirirler. Bu Erişim Noktalarının açık noktalarından biri olarak da tartışılmaktadır. Erişim Noktası Cihazlarının kendisine ait hafızaları vardır. İçlerinde gömülü yazılım (Firmware) bulunmaktadır. Bu yazılımlar yeni çıkan standartlara ya da gelişmelere göre güncellenebilir. Erişim Noktası Cihazları içlerinde güvenlik protokolleri bulundururlar. Bunlardan bazıları WEP (Wired Equivalent Privacy) ,WPA (Wi-Fi Protected Access) ve WPA2 (Wi-Fi Protected Access 2)dir. Erişim noktaları istemcilere otomatik olarak IP (Internet Protocol) atayabilir. Hemen hemen hepsi DHCP (Dynamic Host Control Protocol) mekanizmasına sahiptir. Kullanımı çok yaygındır. Kablosuz modem yada yönlendirici ile karıştırılmamalıdır. Evimizde çoğu zaman internete girdiğimiz kablosuz modem yada yönlendiriclerdir. Bunun yanında havaalanında, öğrenci pansiyonlarında, restoranda, kampüste veya otelde genel kullanıma açık kablosuz ağ kullanarak Internet'e kablosuz bağlandığınızda, genellikle bir erişim noktası aracılığıyla bağlanılır.



Şekil 1.16 Kablosuz Erişim Noktası

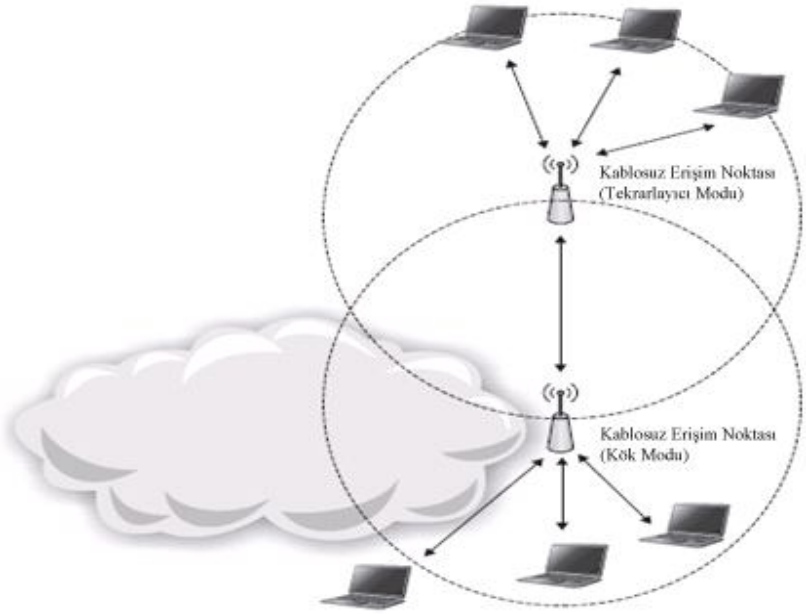
Kablosuz erişim noktaları temel olarak 3 özelliğe sahiptir. Bunlar erişim noktası bu varsayılan(default) modu, diğer ikisi ise tekrarlayıcı (Repeater) modu ve köprü (Bridge) modudur.



Şekil 1.17 Kablosuz Erişim Noktası Kullanım Modları

1.8.3 Kablosuz Tekrarlayıcı (Wireless Repeater)

Tekrarlayıcılar, bit seviyesinde sinyali güçlendiren ve ağın kapsamını genişleten işleve sahip ağ cihazlarından biridir. Telefon, telgraf, mikrodalga, optik haberleşme ve birçok alanda kullanılmaktadır. Kablosuz erişim noktaları da gerektiğinde tekrarlayıcı olarak kullanılabilir. Fakat bir kablosuz ağ ortamında tekrarlayıcı kullanmak için istemci ve interneti alan ana kök erişim noktası bulunması gerekir. Kablosuz ortamlarda kullanılan günümüzdeki AP (Access Point)'ler de konsol uygulaması ile cihazın modunu tekrarlayıcı olarak ayarlamak ve kök AP'nin IP adresini ya da MAC adresini, Tekrarlayıcı olarak kullanılacak AP'nin ayarlarına yazmak gerekmektedir. Tekrarlayıcı kullanılmış bir kablosuz ağ ortamı şekilde görülmektedir.



Şekil 1.18 Tekrarlayıcı Kullanılmış Kablosuz Ağ Örneği

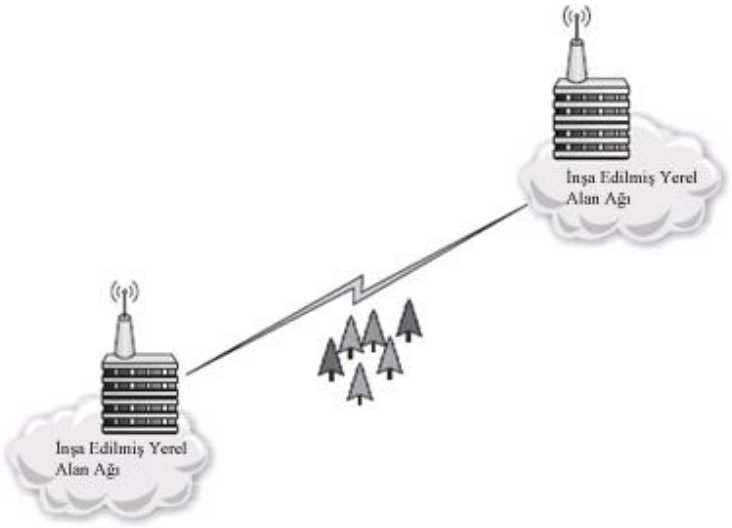
1.8.4 Kablosuz Köprüler (Wireless Bridges)

Köprüler genellikle iki ya da daha fazla LAN ortamını birbirine bağlamak için kullanılırlar. Kablosuz ağlarda genellikle bina dışı (outdoor) uygulamalarda ya da daha opsiyonel LAN'ları bağlamak için bina içi (indoor) ortamlarda kullanılır. İki tip topolojisi vardır. Birincisi Noktadan Noktaya, diğeri ise bir noktadan çok noktayadır.

1.8.4.1 Noktadan Noktaya (Point to Point)

Genellikle Directional ya da SemiDirectional anten kullanılarak bina dışı uygulamalarda iki LAN'ı birleştirerek bir ağ kurarlar. Tipik olarak bağlantılar binadan

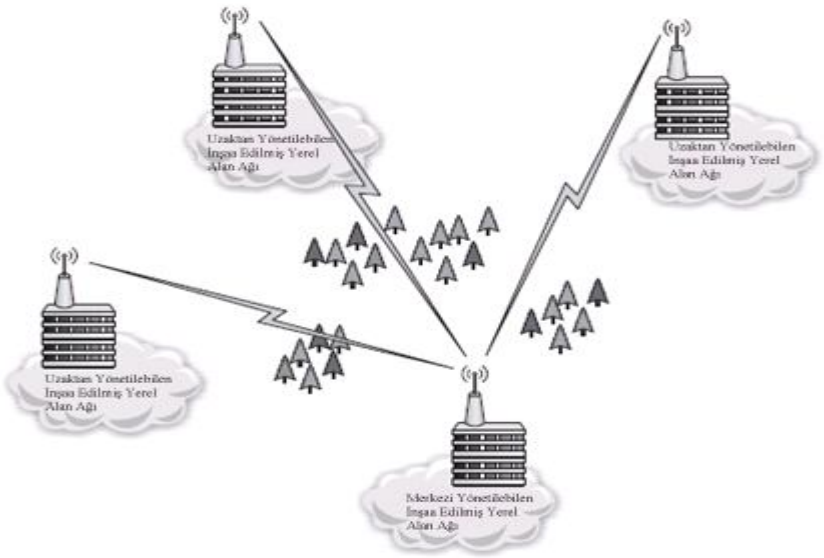
binaya (building to building) ya da siteden siteye (site to site) şeklinde konfigure edilir. Mesafe anten tipine göre en çok 8 km olabilir. Bu mesafede engeller bulunursa bu radyo frekansını kısmen bazen de çok kötü bir şekilde etkileyebilir. Mesafe arttıkça da sinyaller zayıflayacaktır. PtP topolojisi kullanılmış bir kablosuz ortam şekilde görülmektedir.



Şekil 1.19 PtP Topolojisi ile Köprü Uygulaması

1.8.4.2 Noktadan Çok Noktaya (Point to Multi Point)

WAN uygulamalarında daha çok kullanılır. Siteden siteye konfigürasyonu en uygun yapılandırmadır. Semi-omnidirectional ya da yüksek kapasiteli directional antenler kullanılır[Kablosuz Anten Çeşitleri, 2002]. Uzak ağların aynı ağda toplanması için ve özellikle çeşitli ana makinelerin uzaktan bağlantılarında bu topoloji kullanılmaktadır.



Şekil 1.20 PtMP Topolojisi ile Köprü Uygulaması

1.8.5 Kimlik Doğrulama/Yetkilendirme Sunucusu (Authencation Server)

AAA[3] sunucusu olarak ta bilinmektedir. Kablosuz haberleşmede, tasarlı yapıda kablosuz erişim yapmak isteyen kullanıcıların kimlik doğrulama işleminin yapılacağı sunuculardır. Kullanıcı bilgilerinin tutulduğu veritabanını kullanır (Örnek: *Active Directory*), tanımlanmış erişim kontrol listesine göre erişim izni verir/dinamik VLAN (Virtual Local Area Network) ataması yapar. Yetkilendirme sunucusuna erişim istekleri Erişim Kontrol Cihazı üzerinden gelir. 802.1x kullanılması durumunda erişim noktaları erişim kontrol cihazı görevi yapar.

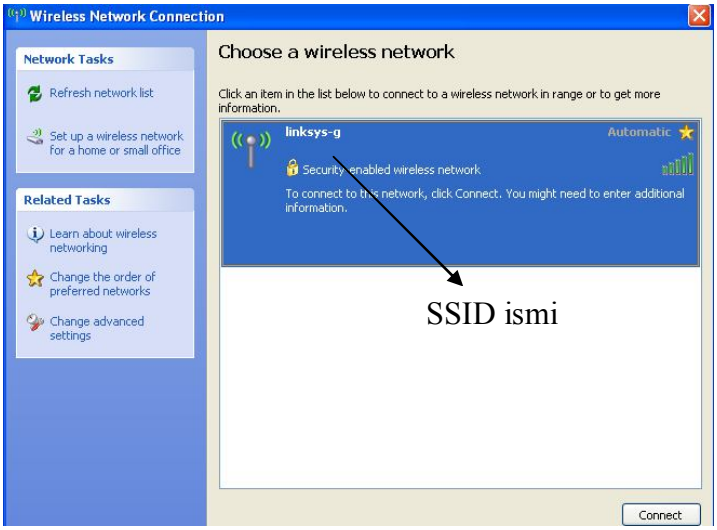
[3] "authorization, authenticated, accounting" bu üç başlıkta belirtilen bölümlerin, bilgilerini tutarak, gelen isteklere cevap veren sunucudur.

2. KABLOSUZ AĞLARDA GÜVENLİK POLİTİKALARI VE ŞİFRELEME

Kablosuz ağların yaygınlığı arttıkça gündeme güvenlik sorunları çıkmaya başlamıştır. Kablosuz Erişim noktaları yâda Modemler broadcast yayın yaptıklarından tüm kablosuz Ethernet yâda kablosuz erişim olan PC ve dizüstüler bu yayını görebilir. Bunun sonucu olarak sisteme izni olmadan giriş yapacak olan saldırganlar, sistemi yavaşlatmak, sistemde bir güvenlik şifresi varsa buna erişmek, sonuç olarak sistemi sabote etmek için denemelerde bulunabilirler. Radyo frekanslarını dinleyip sistem hakkında bilgi sahibi olabilirler. Bunları engellemek amaçlı bazı güvenlik standartları ve politikalar geliştirmiştir. Tezde Kablosuz Erişim Noktalarının içerdiği güvenlik mekanizmaları ve şifreleme yapıları incelenmiştir.

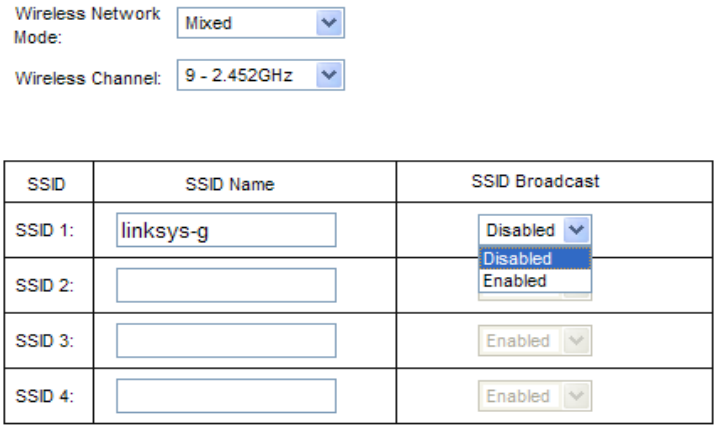
2.1 SSID (Service Set Identifiers) Gizleme

SSID'nin kolay anlaşılması için kablosuz ağ ismi olarak tanımlanabilir. Varsayılan olarak erişim noktalarının adı olarak gelir fakat biz bunu kendi tanımlama ismimizi verebiliriz. Sonuç olarak tarama sonucu gördüğünüz kablosuz ağlarda farklı isimler vardır buna SSID denir. Kablosuz erişim noktaları farklı kanallardan yayın yapabilir. Eğer Erişim Noktasını gizlerseniz sisteme giriş izni olmayan kişiler SSID'yi görmedikleri için bağlantı kurma isteği gönderemezler. Bu konuda uzman olan kişiler 3.parti yazılımlar kullanarak SSID'yi ve hangi kanalda çalıştığını bulabilirler. Ama yinede SSID gizlemek ilk güvenlik basamağımız olarak karşımıza çıkmaktadır.



Şekil 2.1. Gizlenmemiş SSID'li Kablosuz Erişim Noktası Yayını

Şekil 2.1'de bir istemcinin kablosuz olarak çekim mesafesindeki Kablosuz Erişim Noktalarını Windows XP ortamında aradığında çıkan görüntü görülüyor. Böyle açık SSID'li kablosuz erişim noktalarını DoS atakları yapılabilir. Bunun için gizlemekte her zaman fayda görülmektedir. Gizleme işlemi Erişim noktasının cihazının iç yazılımından yapılır.



Şekil 2.2. SSID Gizleme İşlemi

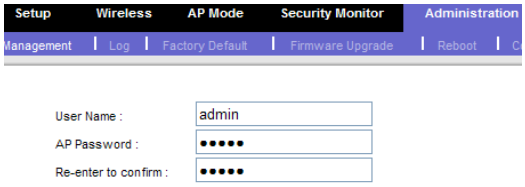
Gizleme işleminden sonra artık kullanıcılar 3.parti bir yazılım ile kullanmadıkları takdirde , Windows Ortamından SSID'yi göremezler. Sisteme izinli kullanıcılar ise SSID ismini bildiklerinde ve şifrelerini girdikleri takdirde ağa otomatik bağlanabilirler.

2.2 Kablosuz Erişim Noktasının Varsayılan Şifresini Değiştirmek

Kablosuz Erişim Noktası satın aldığınızda her firmanın Web arayüzünden cihaza giriş yaparak yönetim yapabileceği bir arayüzü vardır. Sisteme izinli olana kişiler yada şifresiz ağ yapısına sahip olan yerlerde (otel,restoran vb.) kişiler ağ geçidi (gateway) adresini kullarak arayüze girebilirler. Bu girişi engellemek için kablosuz erişim cihazına giriş yapılacak şifreyi değiştirmek güvenlik açısından yapılacak hamlelerden bir tanesidir. Fabrika çıkışı ayarlarda default şifreler vardır. Örnek vermek gerekirse en bilineni user:admin, pass:admin'dir. Erişim Noktası cihazını aldığımızda bu şifreyi değiştirmek gerekmektedir. Değiştirmez isek sisteme giriş izni alan kişiler erişim noktası cihazı ayarlarını değiştirebilir.



Şekil 2.3. WEB arayüzü ile Erişim Noktasına Giriş İşlemi



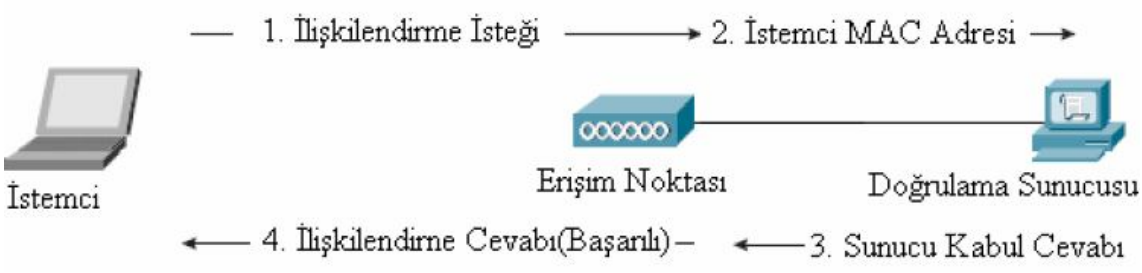
Şekil 2.4. Kablosuz Erişim Noktasının Default Şifresini Değiştirme İşlemi

2.3 Mac Adres Filtreleme (Mac Filtering)

MAC kelimesi Ortam Erişim Yönetimi anlamına gelir ve kısaltma terimini de İngilizce olarak yazılan anlamının yani Media Access Control baş harflerinden almıştır. Fiziksel adres diyede bilinir. MAC adresi her ağ kartına üretici fabrika tarafından atanır. Normal yollarla değiştirilemez ve en önemlisi her ağ kartına farklı bir MAC adresi atanır. MAC adresleri 48 bitlik şifrelere yazılır ve her donanımın ayrı bir MAC adresi vardır, yani şu anda kullandığımız bilgisayarın ağ kartında ve modeminde kendine özel bir MAC numarası vardır. Bu yüzden bir ağ kartları bir diğer ağ kartına veriyi yollarken alıcıyı diğerlerinden ayırmak için MAC adresinden faydalanır. Her ne kadar birbirine denk gelmesi muhtemel iki donanım olsa da, 48 bit çatısı altında üretilen numara, 2 üzeri 48 değerinde yani 281.474.976.710.656 çeşit ağ kartını tanımlamak mümkündür ve bu kadar değer arasında birbirine denk gelmesi muhtemel görülmemektedir. Erişim Noktaları da bu MAC adreslerinden yararlanıp, sisteme giriş yapan istemcilere (client) MAC adresine göre filtreleyerek bir nevi ya dur ya geç der. Bunu için güvenlik kısmında MAC filtrelemeyi etkin hale getirip, sadece erişimine izin verdiğimiz bilgisayarların MAC adreslerini girmeliyiz. Böylece Erişim Noktası sadece bu MAC adreslerine sahip bilgisayarlara erişim verir. Wireless şifresini doğru giren kişinin MAC adresi listede yoksa erişim sağlayamaz. Bir Mac adresi 01-23-45-67-89-ab olarak gösterilebilir. MAC tabanlı doğrulama 802.11 standardında tanımlanmamıstır. Bununla birlikte birçok tedarikçi MAC tabanlı dogrulamayı uyarlamıstır. Tedarikçilerin çogu basitçe, her erisim noktasının geçerli bir erisim kontrol listesi olmasına ihtiyaç duyarlar. Bazı tedarikçiler erisim noktasının merkezi sunucu üzerindeki MAC adres listesini sorgulamasına izin verirler. Erisim kontrol listeleri, kullanıcının sahip oldugu kablosuz ag kartındaki MAC adreslerine göre yapılır. AP'ler, kullanıcının agı kullanmasını bu erisim kontrol listelerine göre sınırlandırırlar. Eger kullanıcının MAC adresi listede varsa ve ağa ulasım için izin verilmisse ağ kaynaklarına erisime izin verilir. Farklı durumda erisim engellenecektir.

1. Kullanıcı erisim noktasına doğrulama istegi gönderir.
2. Erisim noktası, kullanıcının MAC adresini doğrulama sunucusuna gönderir.
3. Sunucu kabul ya da ret cevabını erişim noktasına gönderir.

4. Erişim noktası kullanıcıyı doğrular.



Şekil 2.5. MAC Adresi ile Kimlik Doğrulama



Şekil 2.6. MAC Adres Filtreleme İşlemi

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

2.4 WEP (Wireless Equevileant Privacy) Şifrelemesi

WEP, 802.11 kablosuz ağ güvenlik standartlarındandır. Kablolu ağlarda eşdeğer protokolü geliştiricileri tarafından 802.1 olarak tanımlandı. Tam anlamıyla değişmez Eşdeğer gizliliği olarak ta adlandırılabilir. WEP'in görevi de radyo dalgaları üzerindeki verilerin şifrelenmesini sağlamaktır. Geleneksel kablolu ağ gizliliği ile rekabet edebilmek için tasarlanan WEP, Eylül 1999'da 802.11 standardının parçası olarak onaylandı. WEP gizlilik için Ron Rivest tarafından bulunan RC4 şifreleme algoritmasını ve bütünlük için CRC–32 sağlama toplamını kullanır. WEP' te kullanılan anahtar genişliği olarak 40 ya da 104 bittir.

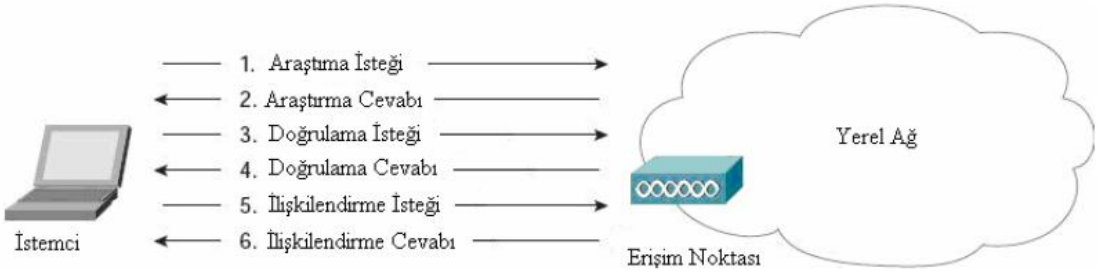
Wep'te şifreleme için RC4 şifreleme algoritması istemcilerde ve Erişim Noktası üzerinde girilen ortak anahtar ile kullanılmaktadır. Fakat günümüzde Linux ya da Windows ortamında bazı yazılımlar ile Ortak anahtar elde ediliyor. Bunun sebebi olarakta RC4 algoritmasının zayıflıkları, Ortak anahtarlar için herhangi bir anahtar yönetim mekanizması bulunmaması, 24-bit Initialization Vector (IV) kullanımının tekrarlanan şifreleme dizilerinin kullanımına yol açması sebepleriyle şifreleme yeterli gizlilik sağlayamamakta, yeterli veri trafiği saldırganlar tarafından kaydedildiğinde paylaşılan anahtar ele geçirilebilmektedir.

2.4.1 WEP'te Kimlik Doğrulama

İstasyon (STA-Station) ile AP arasında ilişkilendirme (Assocation) yapıldığı takdirde veri iletimi yapılabilir. Bunun içinde kimlik doğrulama (Authecantion) işlemi yapılması gerekir.

Wep'te 2 tip asılama vardır. Bunlar açık anahtar kimlik doğrulması, diğeri ise ortak anahtar kimlik doğrulmasıdır.

Bunlardan ilki açık anahtar kimlik doğrulmasıdır. Bu asılamada ilişkilendirme için bir şart yoktur. İsteyen istasyon istediği AP ile iletişime geçebilir.

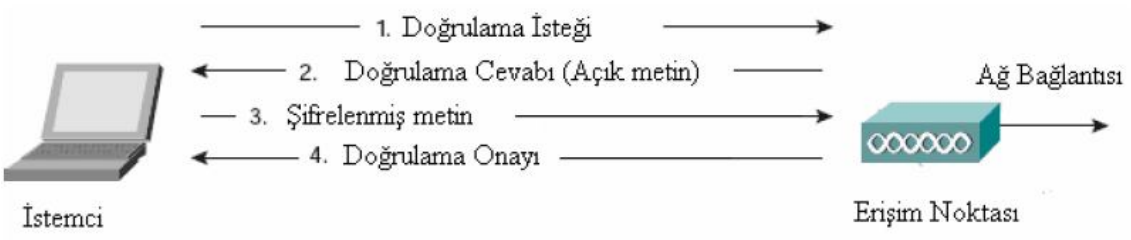


Şekil 2. 7. 802. 11 Açık Anahtar kimlik doğrulaması
[802.1X Port Tabanlı Kimlik Kanıtlama, 2006]

İkincisi ise Ortak Anahtar Kimlik doğrulmasıdır. Bu mekanizmanın çalışması için AP üzerinde aktif hale getirilmesi gerekir. Birde şu bilinmelidir ki WEP'te anahtar dağıtımı ya da yönetimi mekanizması yoktur.

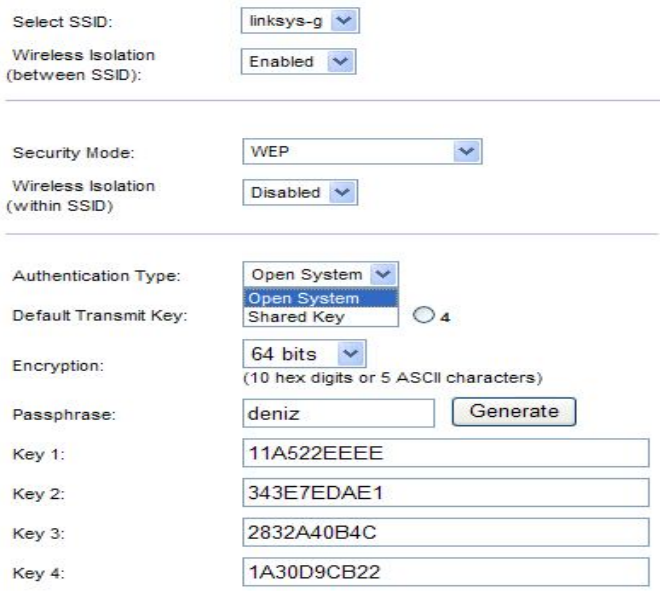
Kimlik Doğrulama şu şekilde yapılır:

1. İlişkilendirilmek isteyen istemci, kimliğini öğrendiği erişim noktasına asıllama isteği gönderir.
2. Erişim noktası bu isteğe karşın bir boş text gönderir. Bunu elindeki anahtar ile istemcinin şifrelemesini ister.
3. İstemci bu texti elindeki şifre ile şifreler ve tekrar AP ye gönderir.
4. AP, aldığı şifreli mesajı elindeki simetrik şifre ile çözer. Ve ilk gönderdiği ile aynı ise işlemi bitirmek için istemciye asıllandığını bildirir.



Şekil 2. 8. Ortak Anahtar kimlik doğrulaması
[802.1X Port Tabanlı Kimlik Kanıtlama, 2006]

5. Bunlardan sonra, istemci ilişkilendirilmek için istek mesaj gönderir. AP'de buna onay mesajı göndererek ilişkilendirildiğini bildirir.



Şekil 2. 9. WEP kullanarak Şifreleme İşlemi

2.4.2 WEP'in Elemanları

Anahtar: WEP, asıllama ve şifreleme işlemlerinde kullanmak için bir ortak anahtar kullanır. WEP'te anahtar uzunluğu default 40 bit ya da 104 bittir.

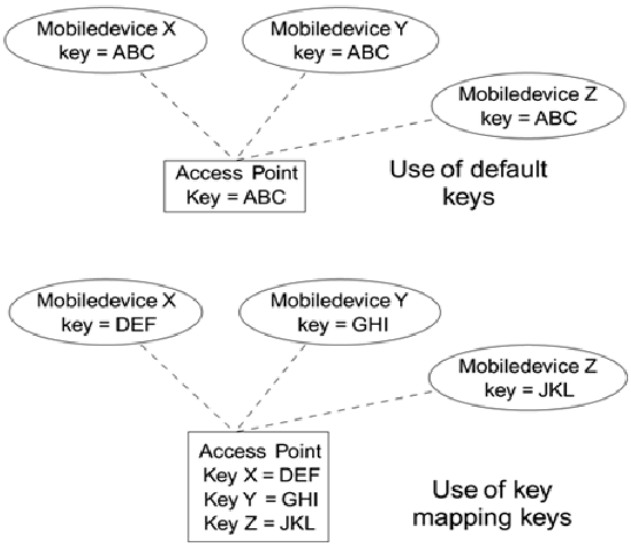
CRC (cyclic redundancy check): Verinin doğru olup olmadığını gösteren kod. Açık Metin için CRC hesaplanarak, açık metnin sonuna eklenir.

Şifreleme Algoritması: WEP, RC4 akış şifreleme algoritmasını ortak anahtar ile kullanarak, yeni bir tek kullanımlık dinamik akış anahtarı elde eder ve açık metini bu akış anahtarı ile XOR'layarak, CRC ekli şifreli metne ulaşır.

Şifre Çözme Algoritması: Şifreleme Algoritması ile aynıdır. RC4 algoritmasını ortak anahtar ile kullanarak, tek kullanımlık dinamik akış anahtarı elde eder ve şifreli metni bu anahtar ile XOR'layarak, CRC ekli açık metni bulur.

Başlangıç Vektörü (IV–Initialization Vector) : Şifreleme İşlemi için kullanılan tek kullanımlık akış şifresini elde ederken, RC4 algoritmasına ortak anahtar ile beraber IV'de parametre olarak girer. Her gönderilecek paket için ayrı ve tek kullanımlık anahtar ile şifrelenerek gönderilir.

2.4.3 WEP'te Kullanılan Anahtarlar



Şekil 2.10 WEP'te kullanılan Anahtar Çeşitleri

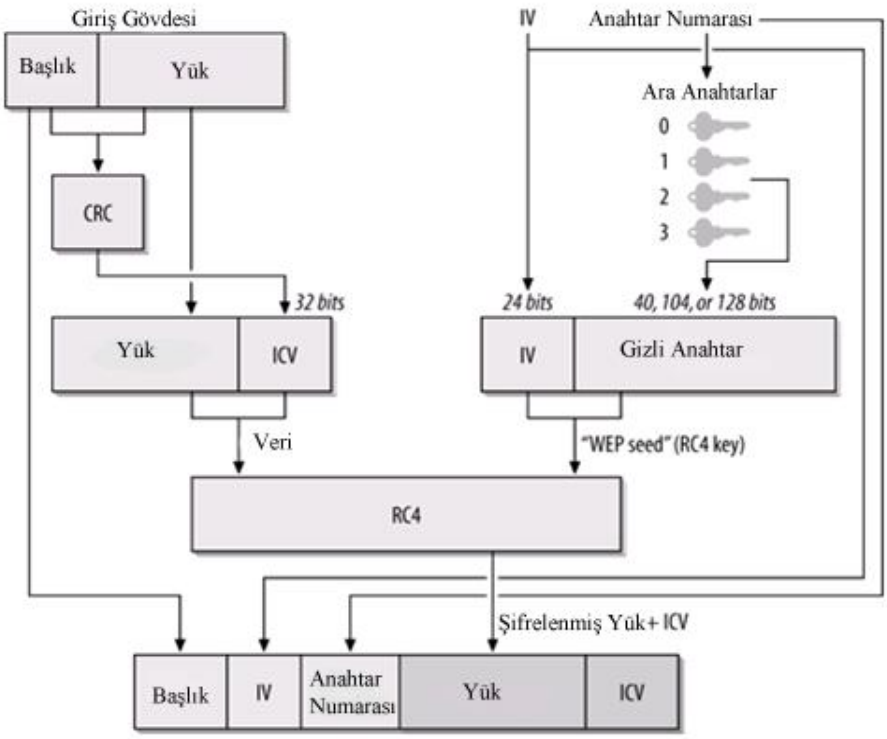
WEP'te kullanılabilecek anahtarlar iki gruba ayrılır. Bunlar ön seçili anahtarlar ve kullanıcıya özel anahtarlardır. Ön seçili anahtarlı yapıda erişim noktası ve

kullanıcılar veri şifrelemede aynı anahtarı kullanır. Açıkça görüldüğü gibi bu yöntem kullanıldığında tüm kullanıcılar tüm verileri çözebilirler. İkinci yöntemde ise erişim noktası her kullanıcıya karşılık farklı anahtarlar bulundurmaktadır bu sayede kullanıcı sadece kendine gelen verileri çözme yeteneğine sahip olacaktır.

2.4.4 WEP'te Veri İşleme

Gizlilik ve Doğrulama Şekil 2.11.'de olduğu gibi aynı zamanda işlenir. Şifrelemeden önce, paket (frame), bütünlük kontrol algoritması'ndan (integrity check algorithm) geçer. Bu algoritma, ICV (integrity check value) denilen hash edilmiş bir değer üretir. ICV, mesaj bütünlüğü için kullanır.

ICV, geçiş işleminde paketin içeriğinin tahriflere karşı ve içeriğin değiştirilmesini engeller, korur. Paket ve bu ICV her ikiside şifrelendi. Bu yüzden ICV tesadüfî saldırganlara kullanışlı değildir.



Şekil 2.11. WEP İşleyişi [Matthew S.,2005]

Giriş olarak, WEP 3 maddeyi gerektirir.

- Payload(yük) korunmak için, şifrelenmek için üst katman protokol yığınlarından gelir.
- Gizli Anahtar, paket şifrelemesinde kullanıldı. Uygulamaya bağlı olarak, Anahtarlar, Özel karakter katarı veya sayı olabilir. WEP eşzamanlı bir şekilde depolanması için dört anahtara izin verir.
- IV, paket iletiminde gizli anahtar ile birlikte kullanıldı.

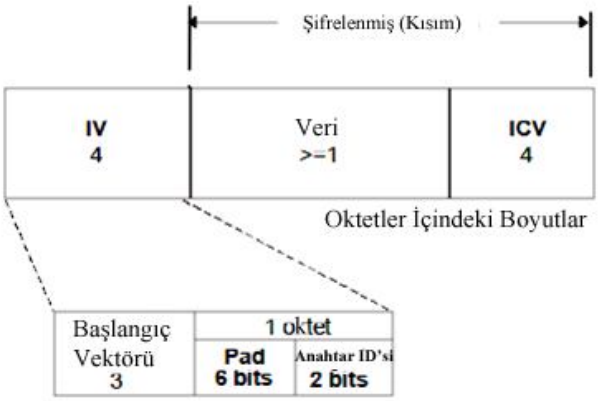
İşlemden sonra, WEP'in tek bir çıktısı vardır.

- Şifrelenen paket, iletildiği noktada çözülmeyi sağlamak için yeterli bilgiyle güvenilmemiş bir şebekenin üzerinde iletim için hazırdır.

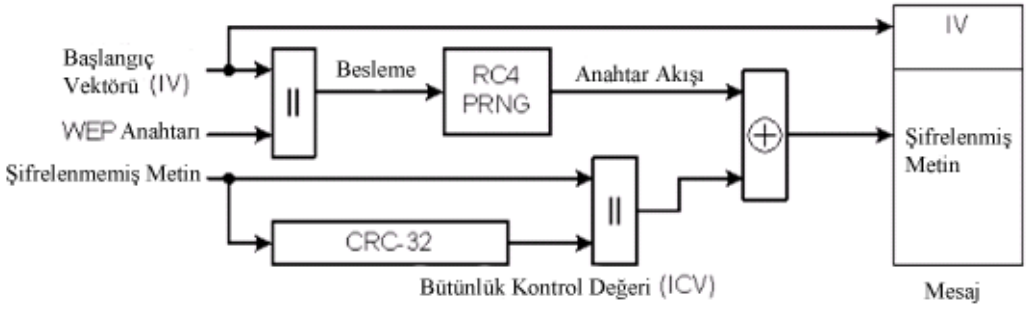
Veri iletimini birde adımlar halinde göstermek istersek;

- 802.11 paketi, iletim için kuyrukta sıralanır. Bu frame payload ve frame başlıklardan oluşur. WEP sadece 802.11 MAC yükünü korur ve buna ek olarak aşağı yani düşük tabakaya bozulmamış bir şekilde 802.11 frame başlıklarını gönderir.
- ICV 802.11 MAC paketinin payload'ı üzerinden hesaplanır. ICV paket payload'nın üzerinden hesaplanır. Bundan dolayı, Snap başlığının ilk bitinden başlar ve ana kısımda en son veri bitine kadar gider. 802.11 frame kontrol sırası henüz hesaplanmadı, bundan dolayı ICV hesabında bulunmaz. WEP tarafından kullanılan ICV, CRC 'dir, sonra üzerinde genişletilecek olan bir noktadır. Bu CRC, açık metnin sonuna eklenir.
- Frame Şifreleme Anahtarı veya WEP Seed bir araya getirilmiştir. WEP anahtarları iki parça ile gelir: Gizli anahtar ve IV (Initialization vector). Akış Şifreleri aynı anahtardan aynı anahtar akışı üretebilecek. Bu yüzden her bir geçiş yapan paket için farklı akış şifreleri üretmek için IV kullanıldı. 40 bitlik Gizli Anahtar ile 24 bitlik IV birbirine eklenerek RC4 algoritmasına sokulur. Bu şekilde RC4 algoritmasına farklı bir anahtar girecektir.

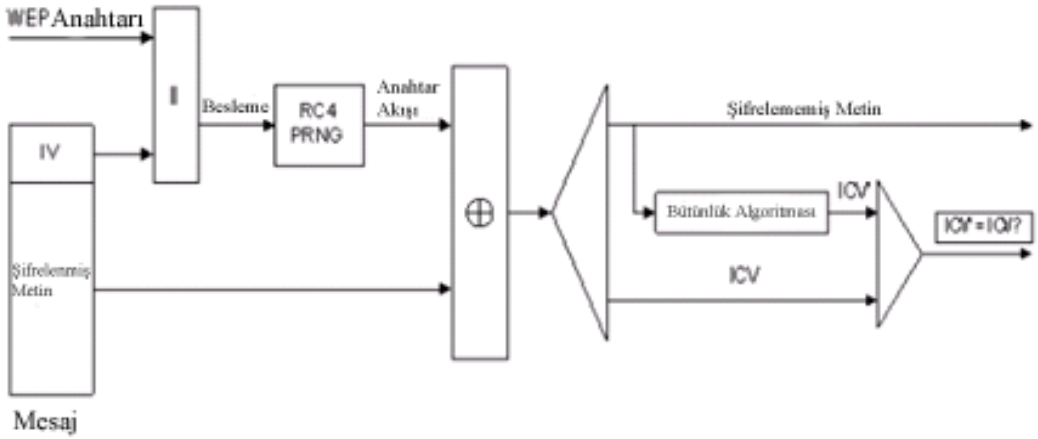
- 64 bit Anahtar, RC4 algoritmasına girdi olur. RC4 algoritması, sahte rastgele sayı üretici ile bir akış anahtarı elde eder. Bu anahtarın uzunluğu, girdi parametresi kadardır.
- Frame şifreleme anahtarı, adım 1'den 802.11 payload'ı ve Adım 2'den ICV'yi şifrelemek için RC4 gibi kullanıldı.
- Elimizde şifrelenmiş payload ile İstasyon iletim için son frame'i toplar. 802.11 başlığı tam alıkoyulur.802.11 Mac Başlığı ve şifrelenmiş payload arasında, WEP başlığı eklendi. Ek olarak IV, Wep başlığı anahtar numarası içerir. WEP 4 adet anahtar ile tasarlanmıştır. Bu yüzden kullanıcı bunu tayin etmelidir. Son başlık toplandıktan sonra, ICV 'nin sonuna başlığın başlamasının giriş MAC Frame üzerine MAC paketi üzerinde 802.11 FCS değeri hesaplanabilir



Şekil 2.12. WEP MPDU Paketi Formatı [Matthew S.,2005]

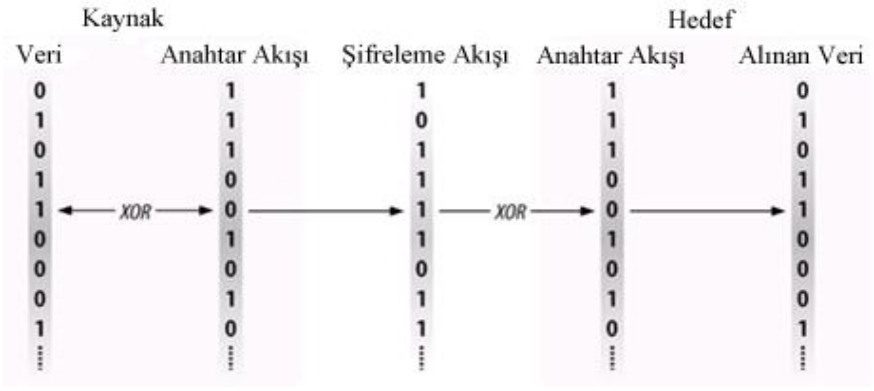


Şekil 2.13. WEP Şifrelemesi Blok Diyagramı [Matthew S.,2005]



Şekil 2.14. WEP Şifre Çözümlemesi Blok Diyagramı [Matthew S.,2005]

WEP, şifreleme işlemini veri bağlantı katmanında simetrik formda bir akış şifresi (stream cipher) olan işte bu RC4 algoritmasını kullanarak yapar. (simetrik şifreleme: encryption ve decryption için aynı anahtarın kullanılması; stream cipher: verinin sabit uzunluktaki bloklar halinde değil işlenirken şifrelenmesi anlamına gelmektedir.). Veriyi korumak, simetrik akış şifrelemesi diye de bilinen RC4 şifrelemesini kullanmayı gerektirir. RC4 tüm akış şifreleri ile özelleiklerinin numarasını paylaşır. Genellikle konuşurken, akış şifrelemesi, bir bitlerin akışını kullanır ki buna keystream denir. Keystream, Chipertext i oluşturmak için mesajla birleşmelidir. Aynı mesajı oluşturmak için şifreli metni keystream ile aynı işleme tabi tutar. RC4 bunun için XOR işlemini kullanır. Burada bir bit 1 oldu mu 1 olur diğerleri 0 bitini oluşturur. Aşağıdaki şekilde bunu gösterir [Tews E.,Weinmann R., Pyshkin A.,,2007].



Şekil 2.15. Akış Şifreleme İşlemi [Matthew S.,2005]

2.4.5 WEP'in Zayıflıkları

Kablosuz ağlar, kablolu ağlara göre daha az güvenlidir. Bunun sebebi kablosuz ağ kartları verileri havadan transfer ettikleri için yetkisiz kullanımlara ve dinlemeye açıktır. Bir ağ koklayıcısı(sniffer) aygıt kullanılarak kablosuz bir ağda gerçekleştirilen iletişim kablolu bir ağa göre çok daha kolay bir şekilde izlenebilir ve çalınabilir.

Kablosuz ağa saldırı gelen saldırıları engellemeyi denemek için, standarda WEP kullanılmıştır. WEP'in önceki bölümde teorik olarak yapısı ve işleyişi açıklanmıştır. Özet olarak bu protokolün ana fikri ağdaki gizliliği sağlamaktır. İkinci fonksiyonu ise kablosuz ağa yetkisiz girişi engellemektir. Fakat yapılan çalışmalar bu protokolün aşağıdaki saldırılara açık olduğunu göstermiştir.

- İstatistiksel analizi taban alan trafiği çözmek için pasif saldırılar.
- Yetkisiz mobil istasyonlardan ağa yeni trafik sokmaya dayalı aktif saldırılar.
- Trafiği çözmek için erişim noktasını kandırmaya dayalı aktif saldırılar.
- Gerçek zamanlı trafiği otomatik olarak çözmek için, bir günlük trafiğin izlendiği ve analiz edildiği bir sözlük oluşturma saldırısı.

Bu şifreleme yöntemindeki problem aslında şifreleme algoritmasının merkezindedir. WEP, RC4 algoritmasını kullanır. Stream Cipher kısa bir anahtarı sonsuz sayıda gelişigüzel anahtar sıralamasına genişletir. Gönderici bu anahtar sırasını göndereceği metin ile XOR'lar (XOR - Exclusive or - Ayrıcalıklı veya) ve şifrelenmiş metni üretir. 2 bit veriyi XOR fonksiyonuna tabi tuttuğunuzda karşılaştırılan iki bitten biri 1 ise (ancak ikisi birden 1 olmayacak) sonuç 1, aksi takdirde sıfır çıkar. Bu yöntemi aklında tutan alıcı şifreli metni çözmek için anahtarın kendisindeki kopyasını kullanır. Alıcıdaki şifreli metin anahtar akışı ile XOR'lanınca orijinal metin elde edilir.

Bu yöntemle çalışan "Stream Cipher"lar kendilerini birkaç saldırı türüne açık ederler. Bu saldırılardan biri ağdan çalınan bir paketteki bir biti değiştirmektir. Bu biti değiştirdiğinizde, veri çözüldüğünde hata çıkmaktadır. Diğer saldırı ise bütün düz

metinleri elde etme imkânına sahiptir. Bu saldırıda dinleyen saldırganın aynı anahtar ile şifrelenmiş iki metni elde etmesi yeterli olmaktadır. Bunu yaparak iki düz metnin XOR'u ele geçirilmiş olur. Bu XOR bilindiğinde istatistiksel saldırılar ile düz metinler çözülebilmektedir. Paylaşılan bir anahtarın ele geçirilen şifreli metinlerinin sayısı çoğaldıkça saldırı daha da kolaylaşmaktadır. Tek bir düz metin çözüldükten sonra diğerlerini çözmek gayet kolaydır.

WEP'in bu iki saldırıya karşı bazı savunmaları vardır. Paketin transfer esnasında değişmediğini garantiye almak için pakette bir Bütünlük Kontrolü (IC - Integrity Check) alanı bulunuyor. Initialization Vector (IV - Başlangıç Vektörü) kullanılarak aynı anahtar dizisiyle iki metnin şifrelenmesi engellenir. Ancak araştırmalar bu önlemlerin hatalı uygulandığını ve bu yüzden güvenlik tedbirlerinin etkisinin azaldığını göstermektedir.

IC (Bütünlük Kontrol) alanı bir CRC-32 sağlaması (çok sık kullanılan bir hata tespit şeması) olarak uygulanır. Bu şemanın problemi lineer olmasıdır. Veri paketleri arasındaki bit farkını temel alarak iki CRC arasındaki bit farkını hesaplamak mümkündür. Bunu yaparak bir saldırgan ağa göndereceği paketteki hangi bitleri değiştireceğini ve paketi kabul edilebilir hale getireceğini tespit edebilir.

WEP algoritmasının diğer bir zayıflığı ise 24-bit Başlangıç Vektörü (IV) kullanmasıdır. Bu, mümkün olabilen IV'lerin sayısını çok düşürmektedir. Yani görece olarak kısa bir süre sonra aynı anahtar dizisinin tekrarlanması mümkün olur. Başka bir sorunda mobil aygıtlar aynı anahtarı kullandığında, IV çarpışma olasılığı da gittikçe büyümektedir.

Bu yüzden WEP şifrelemesinden sonra WPA ve WPA2 şifreleme yapıları geliştirilmiştir. Tezimizde WEP şifresinin kırılması uygulaması incelenmiştir.

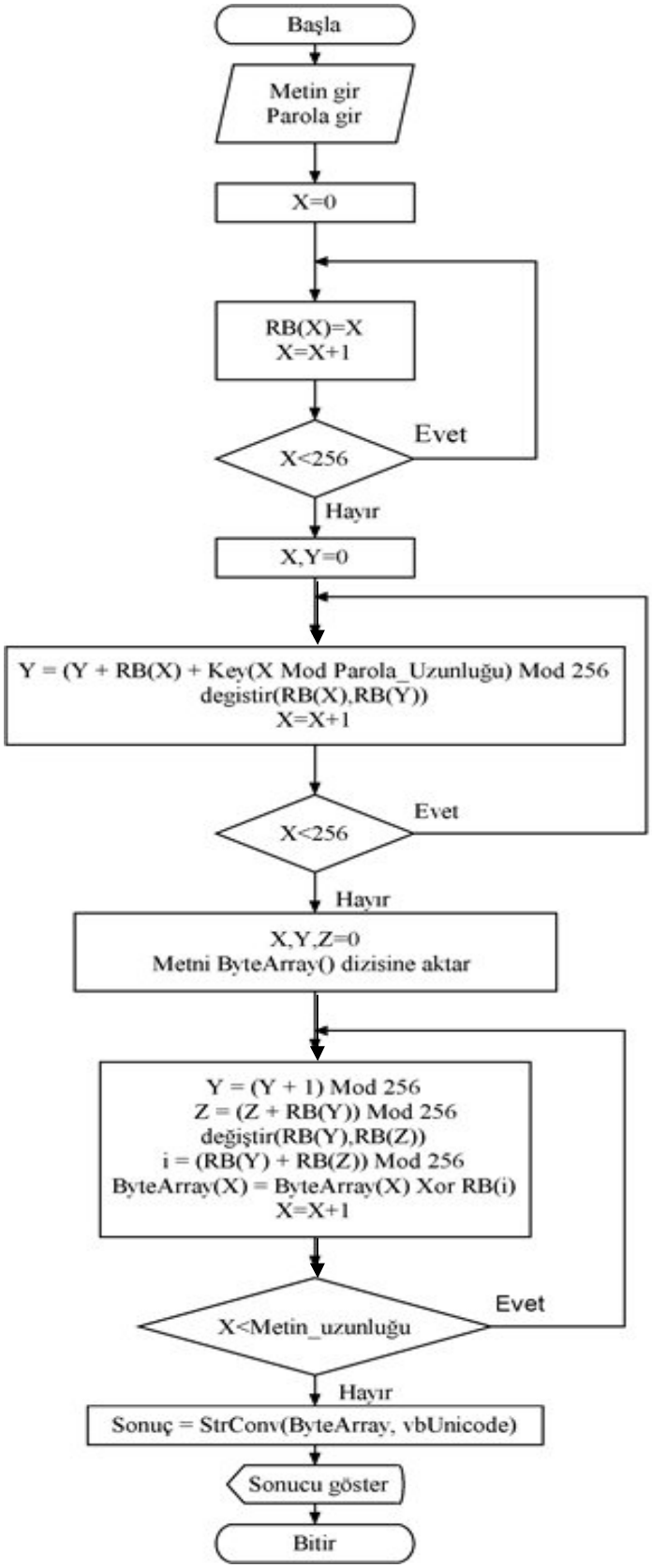
2.4.6 RC4 Şifreleme Algoritması

RC4 (Rivest Cipher 4) şifreleme algoritması 1987 yılında RSA'da çalışan Ronald Rivest tarafından geliştirilmiştir. RC4 akış (stream) şifreleme yöntemini

kullanan bir simetrik şifreleme algoritmasıdır[Fluhrer S,Martin I.,Shamir A.,2001]. Veriyi şifrelemek ve çözmek için aynı anahtarı kullanır. RC4 şifreleme algoritması 1994 yılında bir kişi tarafından internetteki haber gruplarına sızdırılmıştır. Bu algoritmayı kullanabilmek için RC4 olarak değil de başka isimle kullanmak gerekir. Bu yüzden RC4 genellikle ARC4, ARCFOUR (Alleged RC4) olarak kullanılmaktadır.

2.5 WPA (Wi-Fi Protected Access) Şifrelemesi

WEP standardında RC4 algoritmasının açıklarını kapatmak için Wi-Fi Alliance ara geçiş olarak WPA standardını oluşturmuştur. WPA, TKIP'yi desteklemektedir ve TKIP (Temporal Key Integrity Protocol- Tekli şifrelemede Geçici Anahtar Bütünlüğü Protokolü) güçlü bir şifreleme sistemi olarak WEP'in yerini almıştır. TKIP şifreleme işlemlerini gerçekleştirmek için varolan kablosuz aygıtların hesaplama olanaklarını kullanan yeni bir şifreleme algoritması kullanır. TKIP ayrıca şifreleme anahtarları belirlendikten sonra güvenlik yapılandırmasının doğrulanması, her çerçeve için tek noktaya yayın şifreleme anahtarının eşzamanlı olarak değiştirilmesi, önceden paylaşılan her anahtar kimlik doğrulamasının benzersiz olarak başlatılmasının belirlenmesi gibi özellikleri de sağlar. WPA'da Anahtar uzunluğu olarak 128 bit kullanılır. WPA'da anahtar her oturum ve her paket için değişir, dolayısıyla daha yüksek bir güvenlik elde edilmiş olur. WPA'da anahtar yönetimi için 802.1x kullanılır. Kimlik doğrulama için WPA, 802.1x EAP ile güçlü bir yöntem kullanılmıştır. WEP' te veri bütünlüğü ICV ile sağlanırken, WPA' da daha güçlü olan MIC (Message Integraty Code) mekanizması ile sağlanır. WPA uzun vadeli çözüm değildir. Çok Güvenli Ağ (RSN - Robust Secure Network) elde etmek için donanım CCMP'yi desteklemeli ve kullanmalıdır. CCMP'nin yerine TKIP kullanan RSN'ye Geçiş Güvenlik Ağı'da (TSN - Transition Security Network) denir. RSN'ye WPA2 de denir, bu sayede piyasanın aklı karışmaz. WPA kimlik doğrulama/yetkilendirme için iki seçenek sunmaktadır[WPA,WPA2 white Paper,2005].



Şekil 2. 16. RC4 Algoritması Akış Şeması

802.1x kimlik doğrulama/yetkilendirme işlemi sonucunda haberleşme için kullanılacak şifreleme anahtarı istemci ve RADIUS/TACACS sunumcu tarafından karşılıklı olarak oluşturulur ve erişim noktasına RADIUS/TACACS sunumcu tarafından iletilir. Şifreleme için Temporal Key Integrity Protocol (TKIP) kullanılmaktadır. TKIP protokolü, mevcut ürünlerin donanımında herhangi bir değişiklik yapmadan, sadece yazılımsal değişiklik yaparak güvenli veri transferini sağlamak maksadıyla geliştirilmiştir. Bu nedenle, altta WEP'i kullanır. WEP'in açıklarını ve zayıflıklarını yok edecek şekilde güvenli veri transferini gerçekleştirmek için önlemler alınmıştır. Bu nedenle WEP'in etrafında bir kabuk görevi görür. Bu nedenle de, CCMP'ye göre daha fazla işlem yaptığından, güvenlikten çok kullanıcılara zorluk çıkardığı görüşü hâkimdir. TKIP yapısında, WEP'te kullanılan şifreleme algoritması RC4 kullanılmakta, fakat WEP'ten farklı olarak her bir pakette şifreleme anahtarını değiştirilmekte ve IV uzunluğu 24 bit yerine 48 bittir. TKIP, WEP'in bilinen zayıflıklarını kapatmak üzere geliştirilmiş bir yapıdır, WEP'ten TKIP'a donanım değişikliği olmadan geçişe imkân verebilmek amacıyla zayıf bir şifreleme algoritması olan RC4 kullanımına devam edilmiştir. Erişim noktaları ve istemci ağ bağdaştırıcılarının yeni nesil şifreleme algoritması olan AES'in donanımsal olarak desteklemediği durumlarda kullanılabilecek en güvenli şifreleme seçeneğidir. Kurumsal kablosuz ağlarda 802.1x ile birlikte kullanımı gereklidir, WPA-PSK ile kimlik doğrulama yapılması durumunda şifreleme anahtarlarının oluşturulduğu yöntemdeki zayıflık şifreleme yapısının sağladığı gizliliği ortadan kaldırabilir.

TKIP, RC4 akış şifreleyici algoritma üzerine kuruludur.4 yeni algoritma ile WEP şifreleme mekanizmasını sarar.

- IV 48 bite çıkarılmıştır. IV hem paketlere sıra numarası vermek, hem de her paket için tek kullanımlık anahtar üretmede kullanılmaktadır.
- Paketlere sıra numarası verilmesi tekrar(replay) Saldırılarını önlemektedir, hem de sırasız gelen paketlerin atılmasını sağlamaktadır.
- 48 Bitlik IV ve aynı TK(ana anahtar) ile üretilecek tek kullanımlık anahtarlar 100 yıl sonra tekrarlanır.
- Her paket için kullanılan IV değeri TKIP'te değişmektedir. Bu da Zayıf anahtarları önlemektedir.

- Yeni bir mesaj bütünlük kontrol mekanizması MIC (Micheal) (Message integrity check)
- Anahtar eldesi ve dağıtımı ile yeni bir metot getirir.(802.1x)
- Her çerçeve için yeni bir anahtar oluşturulur.

Bu değişiklikler sayesinde kırılamayan bir mekanizma oluşturulması hedeflenmiştir.

Veri bütünlüğü için Michael olarak adlandırılan, paketlerin veri kısmı özetinin (hash) TKIP ile şifrelenmesi yöntemi kullanılmaktadır. Veri bütünlüğü için kullanılan anahtar, veri şifreleme anahtarından farklıdır ve 802.1x kimlik doğrulama aşamasında oluşturulmaktadır.

2.5.1 TKIP (Temporal Key Integrity Protocol)

WPA'da kullanılan yeni şifreleme protokolü TKIP'tir. TKIP 'in geliştirilmesindeki en büyük etken, WEP tabanlı donanımın güvenliğinin arttırılması ve güncellenmesidir. Genel olarak, WEP kullanan donanımların yonga setleri RC4 şifreleme için donanım desteği sağladı. Donanıma yoğun uygulanan şifreleme ile yazılım donanım ve firmware güncellemeleri geri kalanını mümkün kılmıştır. TKIP, WEP'in temel yapısına ve işlemlerine sahiptir. WEP tabanlı çözümlere karşılık bir yazılım güncellemesi olarak tasarlanmıştır. Esas olarak WEP kusurlu olarak gösterildiği için protokol onu WEP'ten ayırabilmek için yeniden adlandırılmıştır. TKIP yukarıda belirtildiği gibi RC4 akış şifrelemesini de kullanır. Sebebi WPA tam bir güvenlik standardı olarak gelişmemiştir. WEP'in açıklarını kapatmak için WEP 'te kullanılan donanımları değiştirmeden güncelleme ile WPA' ya geçişi sağlanmıştır. Bir saldırıya karşı WEP'in zayıf noktalarını savunabilmek için, TKIP çok çeşitli yeni protokol özellikleri ile işbirliği yapar. TKIP, WEP in temel mimarisi ve işlemlerine sahiptir. Ama ayrıca WEP 'in en zayıf noktalarına "Güvenlik Zinciri" ekler.

WEP'ten farklılıkları aşağıda sıralanmıştır.

- Anahtar hiyerarşisi ve otomatik anahtar yönetimi(802.1x):

Wep'te anahtar yönetimi olmadığı için, anahtarı saldırganların çözmesi ve ele geçirmesi kolaylaşmıştır. Bunun için 802.1x anahtar yönetimi mekanizması ile anahtar dinamik hale gelmiştir.

- Frame (Çerçeve) başına anahtarlama:

TKIP, WEP'in RC4 tabanlı frame şifrelemesi sağlamasına rağmen zayıf WEP anahtarlarına karşı saldırıları azaltmak için her frame için ana anahtardan tek bir RC4 anahtarı türetmektedir. Her bir anahtar için, tek bir anahtarın türediği sürece anahtar karıştırma denir.

- Sıra Sayacı:

Her bir frame'i sıra numarası vererek, saldırı durumunda saldırganların geçerli trafiği ele geçirmeleri ve daha sonra yeniden iletme durumunda cevap saldırılara karşı hafifleterek servis dışı frameler etkisiz hale getirilebilir.

- Yeni mesaj Bütünlük Kontrolü (Message Integrity Check -MIC) :

TKIP, Michael da denilen daha güvenli kriptografik bütünlük kontrol hashing algoritmasını kullanarak, WEP'in doğrusal hash'inin yerini alır. Frame hırsızlığını tespit etmek için daha güvenli hashing bunu kolaylaştırır. Ek olarak kaynak adres bütünlük kontrolü ile korunan parçalar arasındadır. Böylelikle belli bir kaynaktan geldiğini iddia eden çalınmış frameleri tespit etmek mümkündür.

- Mesaj bütünlük kontrol hatalarındaki karşı önlemler:

TKIP, varolan donanım üzerine uygulanmak için tasarlanmıştır ve bir sürü kısıtlamadan etkilenmektedir. Michael göreceli kolaylıkla aktif saldırı durumunda tehlikeye girebilir. Böylelikle TKIP aktif saldırından gelen zararları sınırlandırmak için karşı önemleri içermektedir.

- Zayıf Anahtarlar kullanılmamaktadır.
- IV 48 bite çıkarılmıştır:

IV (Initialization Vector) hem paketlere sıra numarası vermek, hem de her paket için tek kullanımlık anahtar üretmede de kullanılmaktadır. 48 Bitlik IV ve aynı TK (Temporal Key) ile üretilecek tek kullanımlık anahtarlar 100 yıl sonra tekrarlanır. Her paket için kullanılan IV değeri TKIP'te değişmektedir. Bu da Zayıf anahtarları önlemektedir.

- Anahtar uzunluğu 128 bite çıkarılmıştır.

Bu değişiklikler sayesinde kırılamayan bir mekanizma oluşturulması hedeflenmiştir [Gezgin D. Buluş E,2009].

2.5.1.1 TKIP' de Veri İşleme ve Çalışma Prensibi

WEP gibi, TKIP, aynı sürecin parçası olarak şifreleme ve bütünlük koruması için destek sağlar. TKIP'in tasarımı emniyetin bir takımı olarak ortaya çıkmıştır. WEP'in etrafında bir çember olarak WEP'i desteklediği tamamen açıktır.

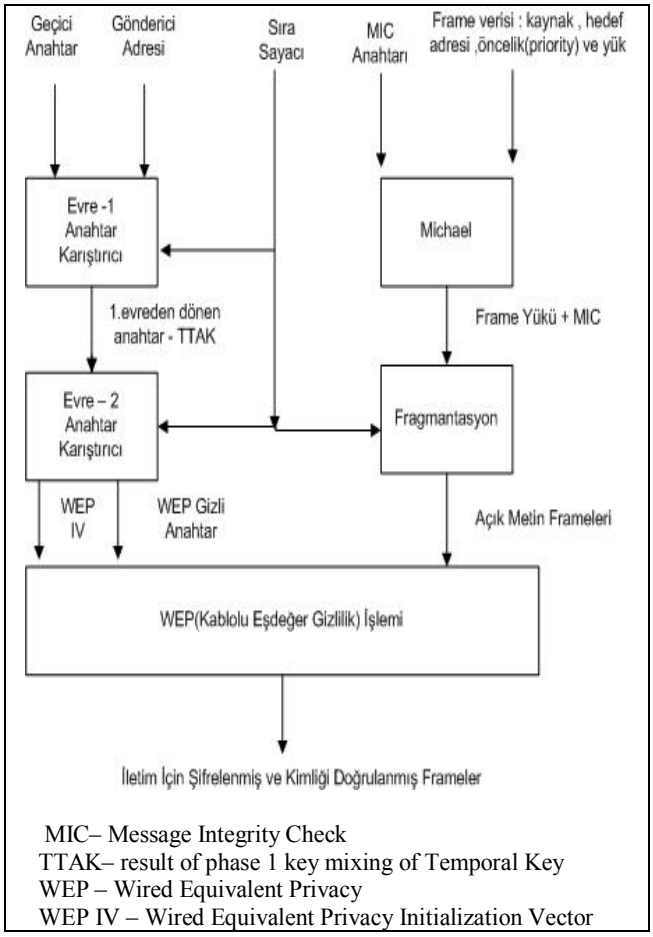
Giriş olarak, TKIP, takip eden maddeleri içerir.

Frame ve Geçici anahtar (Temporal Key), frame'i şifrelemektedir.

Bir MIC anahtarı Michael'le, yapı içeriğini korurdu. TKIP, anahtarların bir çiftini öyle türetir ki istemciden AP(Access Point -Erişim Noktası)'ye MIC anahtarı ile AP'den istemci arasındaki MIC anahtarından farklıdır. TKIP'in, WEP'den ayrıldığı en önemli noktalardan biri, MIC'in, bir anahtar kullandığıdır.

Verici adresi, TKIP'e bir giriş olarak kullanılır çünkü kaynak belgelemesini yapmak için gereklidir. Verici adresi, frame ile sağlanır ve daha yüksek seviye yazılım ile sağlanmaya ihtiyaç duymaz.

Bir sıra sayacı, sürücü veya firmware tarafından tutulur.

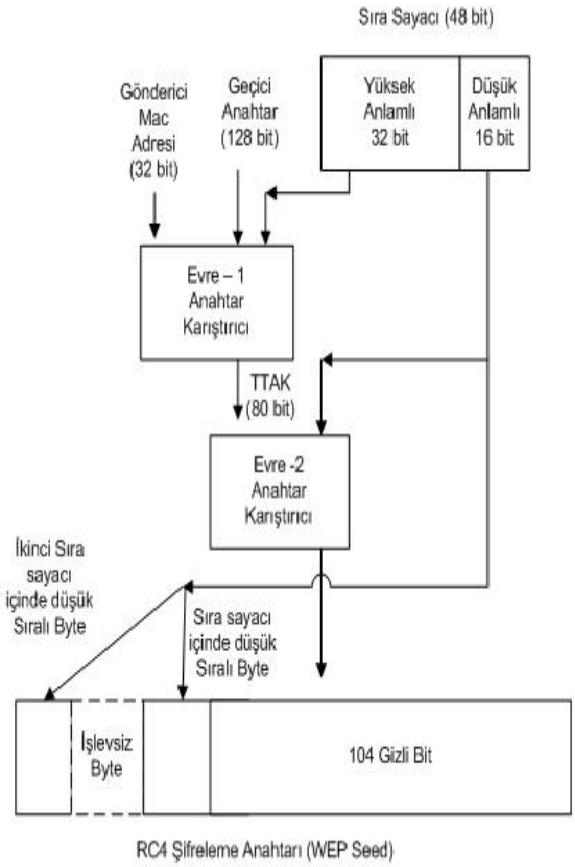


Şekil 2. 19. TKIP Veri Şifreleme İşlemi [Matthew S.,2005]

2.5.1.2 TKIP' de Anahtar Karıştırma İşlemi

WEP'te aynı anahtar ile şifrelenmiş frame dayalı saldırılar yapılabilmekteydi. WPA da bu saldırıları engellemek hususunda her paket için farklı anahtarlar üretilmesi öngörülmüştür. TKIP, her yapı için benzersiz bir anahtar türetir. Anahtar, başa

döndürme vektörü (IV) ,sıra sayacı, frame'in vericisinin adresi ve geçici anahtar ile üretilir. Bu ilk adımda 80 bitlik bir ara anahtar elde edilir. Buna TTAK ismi verilir. Böylece Anahtar karıştırma işlemi anahtarın daha önce kullanılmadığını garanti eder ve herhangi bir saldırıyı engellemektedir. TKIP, karışık anahtarın hesaplamasını ayırır. Evre birde giriş olarak başta belirtildiği gibi verici adresi, 48 bitlik sıra sayacının yüksek anlamlı 32 bitlik parçası (IV) ve 128-bitlik geçici anahtardır. Çıktı olarak ise 80-bitlik bir ara anahtar değerini verir. Anahtar karıştırma görevin evre ikisi, her yapı için hesaplanmalıdır. Giriş olarak, ikinci evre, birinci evrenin verdiğini, geçici anahtar ve sıra sayacının düşük anlamlı 16 bitini alır. Yapıdan çerçevelemek için değiştirilen tek giriş, sıra sayacıdır. Böylece Anahtarlar her oturum, her paket için değişir.



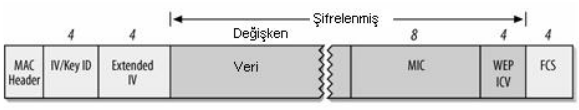
Şekil 2. 20. TKIP Anahtar Karıştırma İşlemi [Matthew S.,2005]

2.5.1.3 TKIP' de Veri İletimi

Bir frame oluşturulduğu ve aktarma için TKIP'e yollandığı zaman, olayların takip eden sırası aşağıdaki gibidir.

1. 802.11 frame'i iletim için kuyrukta beklenir. Frame, bir frame başlığı ve yükü (payload) içerir. WEP gibi TKIP'te, sadece 802. 11 MAC yükünü korur ve 802.11 frame başlığını ile bağlantıyı keser.
2. Mesaj bütünlük kontrolü (MIC), hesaplanır. WEP'den farklı, TKIP'in MIC'i, daha sağlam kriptografik bir algoritmaya sahiptir. O, onun geçerli kılma sürecinin parçasının olduğu gibi gizli bir anahtarı kullanır ve 802. 11 frame yükünden çok daha fazla korur. Yapı verisine ek olarak, MIC, kaynağı birleştirir ve varış yeri, gelecek 802.11e standardı ile kullanılacak olan öncelik parçalarının toplamasına ek olarak hitap eder.
3. Sıra sayacından gelen sayılar, yukarı kısımdan gelen parçalara tayin edilir. WEP başa döndürme vektörlerinden farklı, TKIP'in sıra sayacı, her parça için sayıyı bir artırır.
4. Her frame, WEP anahtarı ile benzersiz şifrelenir. Anahtar karıştırıcılar görevleri tamamlayarak, TKIP'te, WEP anahtarını, her yapı için farklı anahtar üretir. Yapı başına anahtar, bir IV olarak WEP'e gizli bir anahtarla beraber geçilir; Her iki bileşen, her yapı için değiştirilir.
5. İkinci adımdan Michael mesaj bütünlük kontrol değeriyle beraber yapı, ve adım dörtten RC4 anahtarı ile WEP'e geçilir, Buda bize TKIP ile korunan bir yapının da, WEP bileşenlerini kapsayacak olduğunu ifade eder[Tanenbaum A.,2003].

Sonuç olarak aşağıda da TKIP'te kapsüllenmiş bir frame yapısı gösterilmektedir.

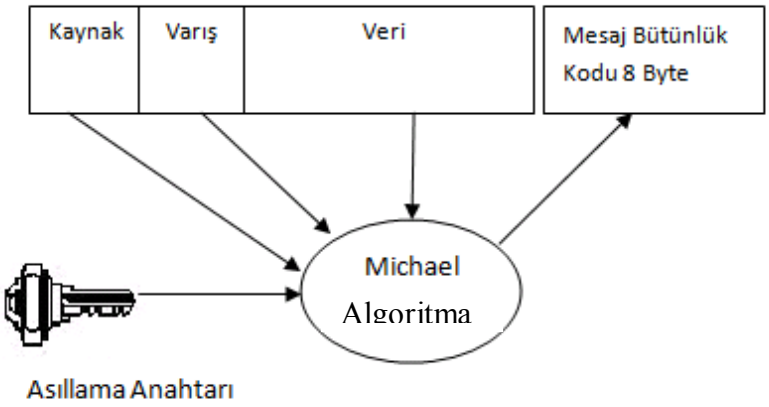


Şekil 2. 21. TKIP Kapsüllenmiş Frame Yapısı[Matthew S.,2005]

2.5.1.4 Mesaj Bütünlük Kontrolü (MIC)

802.11 ve WEP ile veri bütünlüğü 802.11 yüküne eklenen ve WEP ile şifrelenen bir 32 bit bütünlük denetim değeri (ICV) ile sağlanır. ICV şifrelenmiş olsa da, şifrelenmiş yüklerdeki bit değerlerini şifreleme incelemesi kullanarak değiştirebilir ve şifrelenmiş ICV'yi alıcı algılamadan güncelleştirebilir.

WPA ile Michael Algoritması olarak bilinen bir yöntem, var olan kablosuz aygıtlarda kullanılan hesaplama olanakları yardımıyla 8 baytlık bir ileti bütünlüğü kodu (MIC) hesaplayan yeni bir algoritma tanımlamaktadır. MIC, IEEE 802. 11 çerçevesinin veri bölümü ile 4 baytlık ICV arasına yerleştirilir. MIC alanı, çerçeve verileri ve ICV ile birlikte şifrelenir. Michael ayrıca yeniden gönderme koruması sağlar. Yeniden gönderme saldırılarını engellemek amacıyla, IEEE 802.11 çerçevesinde yeni bir çerçeve sayacı kullanılır.

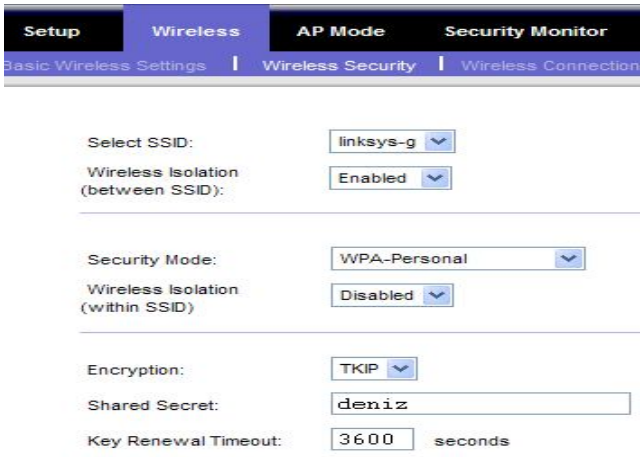


Şekil 2.22. Michael Algoritması [Matthew S.,2005]

2.5.2 WPA'da Kimlik Doğrulama

WPA kimlik doğrulama/yetkilendirme için iki seçenek sunmaktadır.

Birincisi ev kullanıcıları, küçük işletmeler için tasarlanmış olan WPA-PSK yapısıdır. 8–63 karakter arası bir şifre belirlenir. WPA-PSK'da kimlik doğrulama için istemciler ve erişim noktası üzerinde girilen bir paylaşılan parola (PSK) kullanılmaktadır. Paylaşılmış anahtar istemcilerin işletim sisteminde tutulmakta, bu sebeple PSK anahtarı çalınma/kırma saldırıları ile başkalarının eline geçme riski taşımaktadır (Örnek: WzCook saldırı yazılımı, üzerinde çalıştığı işletim sistemindeki anahtarlarını kullanıcıya bildirmektedir.). Kimlik doğrulama trafiğini kaydeden saldırganların sözlük saldırılarına olanak tanıyan bir yapıdır. Tek ortak anahtar kullanımı kullanıcıların ayırt edilebilmesini/ farklı yetkilendirmelerin yapılmasını/ kullanıcı tabanlı kayıt tutulmasını olanaksız kılmaktadır. Ayrıca bir istemci bilgisayarının çalınması durumunda ya da yetkisiz bir erişim olduğunda PSK'nın ele geçmesi muhtemeldir. Kurumsal kablosuz ağlarda kullanımı uygun değildir.



Şekil 2. 23. WPA-PSK Şifrelemesi AP Konfigurasyonu

İkinci seçenek ise 802.1x kullanımıdır. IEEE 802.1x, port tabanlı ağ erişim kontrol mekanizmasıdır ve uzaktan erişim, VPN, anahtarlama cihazı vb. uygulama/birimlerin kimlik doğrulama/yetkilendirme yöntemi olarak kablolu ağlarda kullanılmaktadır. 802.1x erişim kontrolünde yer alan bileşenler: istemci (dizüstü bilgisayarı, PDA, cep

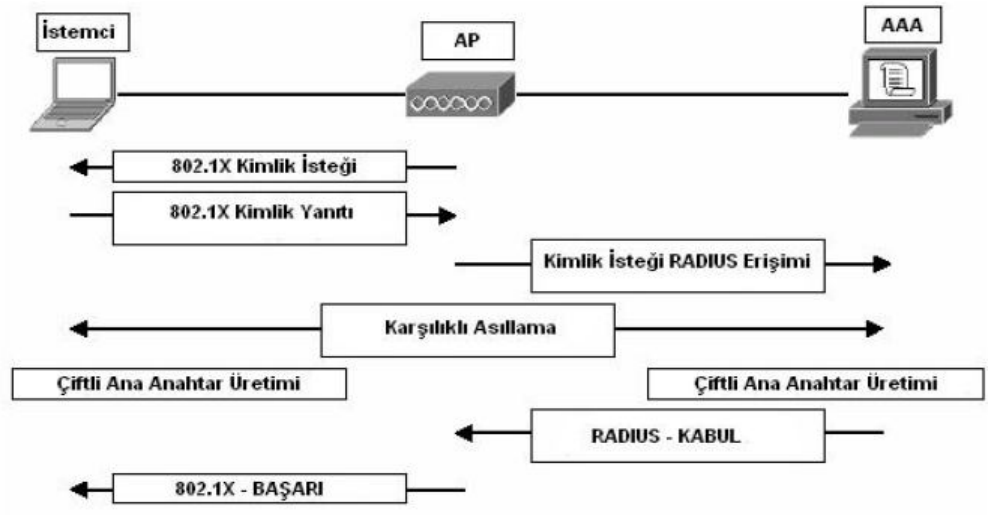
telefonu, PC vb.), erişim noktası ve RADIUS/TACACS erişim kontrol sunucusudur. İstemciler bağlantı isteklerini erişim noktasına bildirirler, erişim noktası isteği RADIUS/TACAS sunucuya yöneltir ve kimlik doğrulama/yetkilendirme işlemini RADIUS/TACACS sunucu [Gezgin D.,Buluş E.,Buluş N.,2009] gerçekleştirerek sonucu erişim noktası ve istemciye bildirir. Sonuca göre erişim noktası istemciye bağlantı için sanal bir port açar. Bu işlemler sonucunda ek olarak erişim noktası ve istemci arasındaki şifreli haberleşmelerde kullanılacak şifreleme anahtarları oluşturulur.

A. 802.1x'te PEAP (kullanıcı hesap bilgileri kullanılarak), EAP-TLS (Sertifika tabanlı), EAP-MD5 (şifre kullanılarak) vb. protokoller kullanılarak kimlik doğrulama işlemi gerçekleştirilebilmektedir.
B. 802.1x ile çift yönlü kimlik doğrulama mümkündür, istemciler ve RADIUS/TACACS sunucusu karşılıklı olarak kimlik doğrulama işlemi gerçekleştirebilirler, böylece istemcilerde doğru ağa bağlandıklarını kontrol edebilirler.
C. 802.1x ile yetkilendirmede erişim politikaları tanımlanabilmekte, ait olduğu etki alanı, kullanıcı grubu, bağlantı türü, bağlantı zamanı, bağlandığı erişim noktası vb. ölçütlere göre yetkilendirme yapılabilmektedir.
D. 802.1x erişim kontrolünde yer alan bileşenler: istemci (dizüstü bilgisayarı, PDA, cep telefonu, PC vb.), erişim noktası ve RADIUS/TACACS erişim kontrol sunucusudur. İstemciler bağlantı isteklerini erişim noktasına bildirirler, erişim noktası isteği RADIUS/TACAS sunucuya yöneltir ve kimlik doğrulama/yetkilendirme işlemini RADIUS/TACACS sunucu gerçekleştirerek sonucu erişim noktası ve istemciye bildirir. Sonuca göre erişim noktası istemciye bağlantı için sanal bir port açar. Bu işlemler sonucunda ek olarak erişim noktası ve istemci arasındaki şifreli haberleşmelerde kullanılacak şifreleme anahtarları oluşturulur.

802.1X Asıllama Adımları:

1. Kullanıcı, asıllayıcıya bağlantı talebinde bulunur. Asıllayıcı, bağlantı isteğini alınca, tüm portları kapalı tutar fakat kullanıcı ile arasında bir port açar.

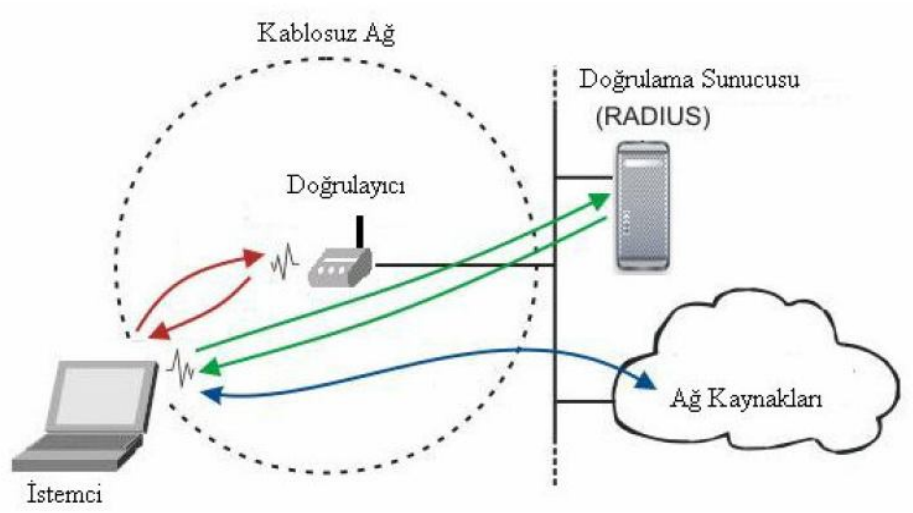
2. Asıllayıcı, kullanıcıdan kimliğini (identity) ister.
3. Kullanıcı kimliğini gönderir. Asıllayıcı kimlik bilgisini bir asıllama sunucusuna gönderir.
4. Asıllama sunucusu, kullanıcının kimliğini asıllar. Asıllandığında, Kabul (accept) mesajı asıllayıcıya gönderilir. Asıllayıcı, kullanıcının portunu yetkilendirilmiş duruma getirir.
5. Kullanıcı, asıllama sunucusundan, onun kimliğini ister. Asıllama sunucusu, kimlik bilgisini kullanıcıya gönderir.
6. Kullanıcı, asıllama sunucusunun kimliğini asıladığında veri trafiğe başlar.



Şekil 2.24. IEEE 802.1X ile Asıllama İşlemi
[802.1X Port Tabanlı Kimlik Kanıtlama, 2006]

802.1X–2001 genel standardı şudur:

"Port tabanlı ağ erişim denetimi, noktadan-noktaya bağlantı özelliklerine sahip bir yerel ağ portuna takılan cihazların kimlik doğrulaması ve yetkilendirme için ve bu sayede kimlik doğrulaması ve yetkilendirmesi başarısız olması durumunda o portu erişimden koruyarak IEEE 802 yerel ağ altyapılarının fiziksel erişim özelliklerinin kullanımına olanak sağlar. Bu bağlamda bir port, yerel ağ altyapısına ekli tekil bir noktadır."



Şekil 2. 25. 802.1X Yapısı
[802.1X Port Tabanlı Kimlik Kanıtlama, 2006]

Bir kablosuz düğümün diğer yerel ağ kaynaklarına erişebilmesi için kimlik kanıtlaması yapılmalıdır.

1. Yeni bir telsiz düğüm (TD) bir yerel ağ kaynağına erişim isterse, erişim noktası TD'nin kimliğini sorar. TD'nin kimliği doğrulanmadan EAP'den başka hiçbir akışa izin verilmez ("port" kapalıdır).

Kimlik kanıtlaması isteyen telsiz düğüme genellikle İstemci denir, aslında telsiz düğümün bir İstemci içerdiğini söylemek daha doğru olur. İstemci güven ortamını oluşturacak Kimlik Kanıtlayıcı veriye cevap vermekle sorumludur. Aynısı erişim noktası için de geçerlidir; Kimlik Kanıtlayıcı erişim noktası değildir. Şöyle ki, erişim noktası bir Kimlik Kanıtlayıcı içerir ama Kimlik Kanıtlayıcı erişim noktasında olmasa da olur; harici bir unsur da olabilir.

Kimlik kanıtlama için kullanılan EAP ilk olarak çevirmeli PPP için kullanılmıştır. Kimlik olarak kullanıcı adı ile birlikte PAP veya CHAP [RFC1994] tarafından doğrulaması yapılacak kullanıcı parolası kullanılır. Kimlik açık (şifrelenmemiş) gönderildiği için kötü niyetli bir dinleyici kullanıcının kimliğini öğrenebilir. O zaman "Kimlik saklama" (Identity hiding) kullanılır; şifrelenmiş TLS tüneli kurulmadan gerçek kimlik gönderilmez.

2. Kimlik gönderildikten sonra kimlik kanıtlama süreci başlar. İstemci ve Kimlik Kanıtlayıcı arasında kullanılan protokol EAP'tır veya daha doğru olarak EAP kaplamalı yerel ağ'dır (EAPOL). Kimlik Kanıtlayıcı EAP iletilerini RADIUS biçimine yeniden dönüştürür ve onları Kimlik Kanıtlayıcı Sunucuya aktarır.

Kimlik kanıtlama süresince, Kimlik Kanıtlayıcı sadece İstemci ve Kimlik Kanıtlama Sunucusu arasında paketleri nakleder. Kimlik kanıtlama süreci bittiğinde Kimlik Kanıtlama Sunucusu başarı (veya doğrulama başarısız olursa, başarısızlık) iletisi gönderir ve Kimlik Kanıtlayıcı "port"'u İstemci için açar.

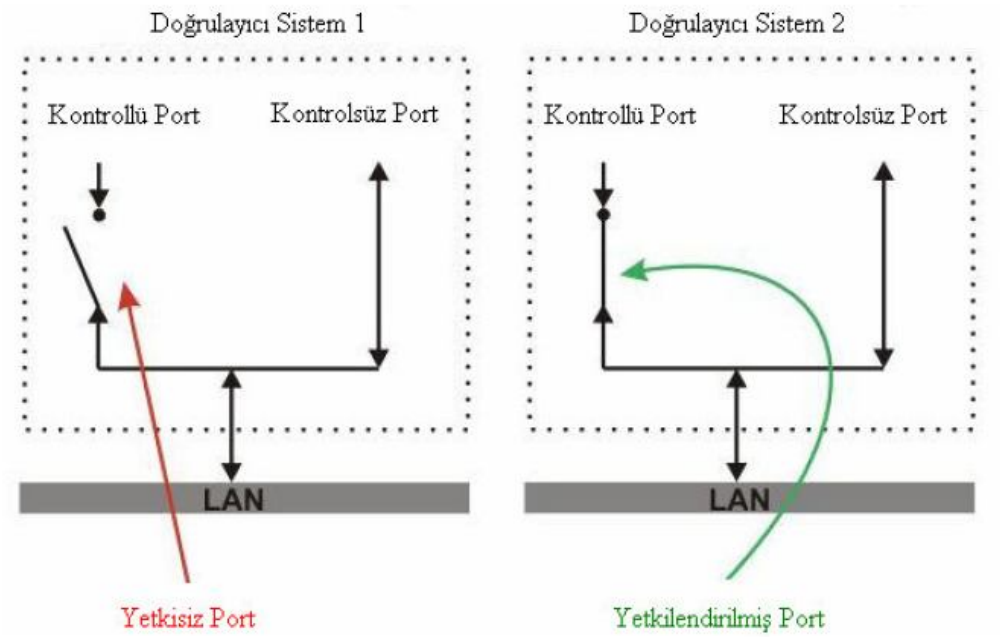
3. Başarılı bir kimlik kanıtlamadan sonra İstemci diğer yerel ağ kaynaklarına/Internete erişmeye hak kazanır.

Neden "port" tabanlı kimlik kanıtlama deniyor? Çünkü Kimlik Kanıtlayıcı denetimli ve denetimsiz portlarla uğraşır. Denetimli port da denetimsiz port da mantıksal varlıklardır (sanal portlar); ama yerel ağa aynı fiziksel bağlantıyı kullanırlar (aynı bağlama noktası).

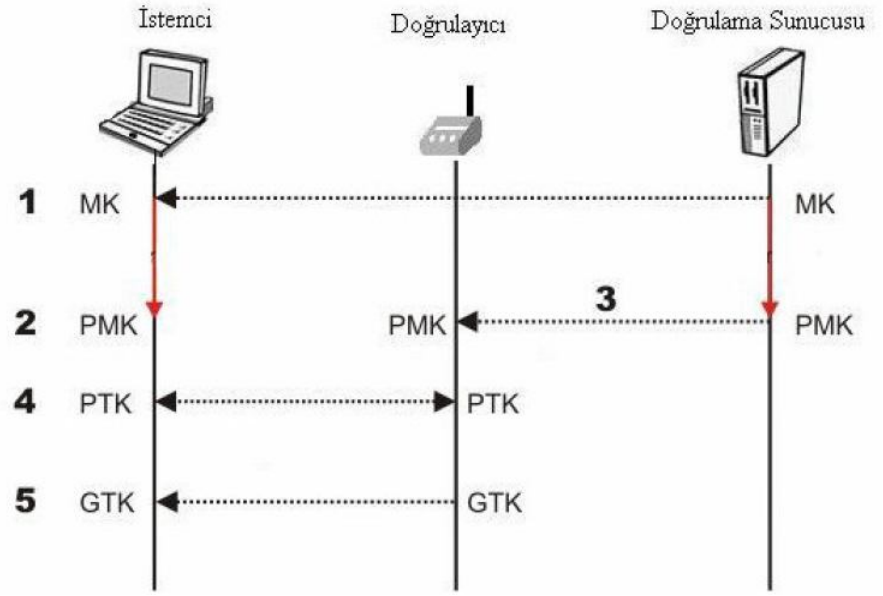
2.5.3 WPA'da Anahtar Yönetimi

Dinamik anahtar değişimi ve yönetimi

Şifreleme ve tümleşiklik algoritmaları kullanarak bir güvenlik kuralları bütünü oluşturmak için anahtarlar kullanılmalıdır. Neyse ki 802.11i bir anahtar türetme/yönetim tarzını içerir (şekil 2.27).



Şekil 2. 26. 802.1X denetimli /denetimsiz port
[802.1X Port Tabanlı Kimlik Kanıtlama, 2006]

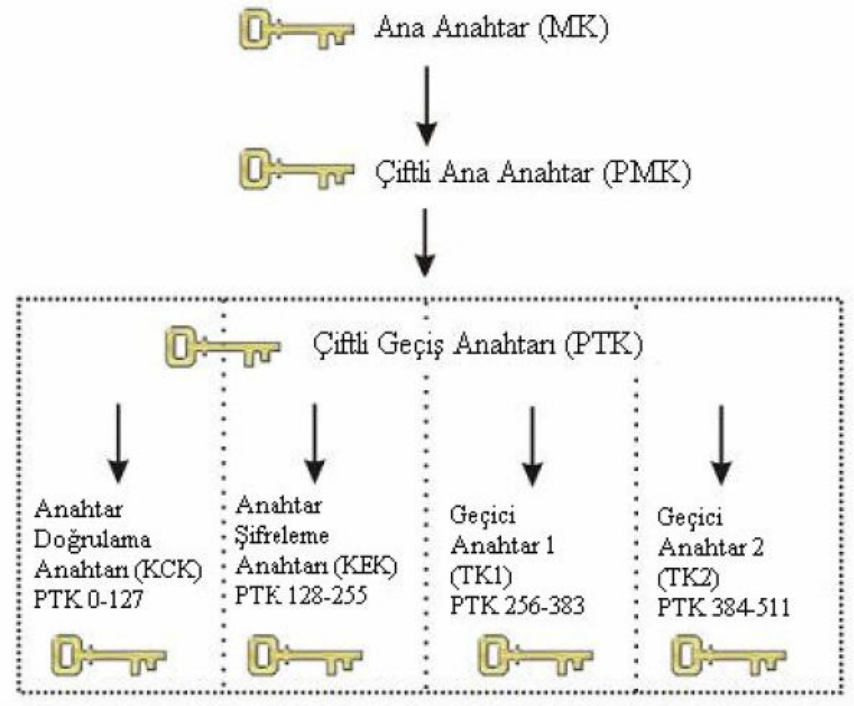


Şekil 2.27. 802.1X Anahtar Yönetimi ve Dağıtımı
[802.1X Port Tabanlı Kimlik Kanıtlama, 2006]

1. İstemci (WN) ve Kimlik Kanıtlama Sunucusu (AS) doğrulama yaparken AS'den gönderilen doğrulamanın başarılı olduğunu söyleyen son iletilerden biri bir Ana Anahtar'dır (MK - Master Key). Gönderildikren sonra MK sadece WN ve AS tarafından bilinir. MK, WN ve AS arasındaki bu oturuma bağlıdır.
2. Hem WN hem AS, MK'dan bir Ana Oturum Anahtarı (PMK - Pairwise Master Key) üretir.
3. O zaman PMK AS'den Kimlik Kanıtlayıcıya (AP) taşınır. PMK'yi sadece WN ve AS türetebilir, bunun yanında AP, AS'nin yerine erişim-denetim kararları verebilir. PMK, WN ve AP arasındaki bu oturuma bağlı yepyeni bir simetrik anahtardır.
4. Ana Oturum Anahtarını türetmek, bağlamak ve doğrulamak için WN ve AP arasında PMK ve 4 yönlü el sıkışma kullanılır. PTK işletimsel anahtarlar topluluğudur:

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

5. KEK ve 4 yönlü grup elşıkışması AS'den WN'ye Grup Geçiş Anahtarını (GTK) göndermek için kullanılır. GTK aynı Kimlik Kanıtlayıcıya bağlı tüm İstemciler (WN'ler) arasında paylaşılan bir anahtardır ve çoğa gönderimli iletişim akışını güvenli kılmak için kullanılır.



Şekil 2.28. Ana Oturum Anahtarı Düzeni
[802.1X Port Tabanlı Kimlik Kanıtlama, 2006]

Önpaylaşımlı Anahtar

Küçük çalışma odaları / evdeki çalışma odaları, amaca-yönelik ağlar veya ev kullanımı için Önpaylaşımlı Anahtar (PSK - Pre-Shared Key) kullanılabilir. PSK kullanırken tüm 802.1X kimlik kanıtlama sürecinde birşeyler eksik olur. EAP (ve RADIUS) kullanan WPA'ya "Kurumsal WPA" veya sadece "WPA" dendiği gibi buna da "Kişisel WPA" (WPA-PSK) denmiştir[Öztürk E.,2004].

2.6 WPA2 (Wi-Fi Protected Access 2) Şifrelemesi (IEEE 802.11i)

IEEE 802.11i çalışma grubu tarafından WEP'in zayıflıklarını tümüyle ortadan kaldırmak amacıyla oluşturulmuş güvenlik standardıdır. WPA2 veya Robust Security Network olarak da bilinmektedir. Advanced Encryption Standard (AES) şifreleme algoritmasının Counter Mode with Cipher Block Chaining Message Authentication

Code Protocol (CCMP) modunda şifreleme ve veri bütünlüğü kontrolü için ve 802.1x'in kimlik doğrulama/yetkilendirme için kullanımını önermektedir. WPA ile aynı yapıyı, 802.1x'i kullanmaktadır. Advanced Encryption System (AES) şifreleme algoritması Counter Mode modunda kullanılmaktadır. Bu yöntemle WEP ve TKIP'te kullanılan IV ve TKIP'te uygulanan her pakete bir anahatar (per packet keying) mekanizmasına ihtiyaç kalmaksızın şifreleme anahtarı tekrarını önleyen bir yapı oluşturulmuştur. AES şifreleme algoritması RC4 algoritmasına göre daha güçlü bir şifreleme algoritmasıdır ve bilinen herhangi bir zayıflık içermemektedir. AES kullanımını desteklemeyen donanımlara yönelik uyumluluk için RC4 şifreleme algoritması kullanan TKIP yapısı da IEEE 802.11i standardında bulunmaktadır. RSN asıllamayı ve anahtar yönetimini IEEE 802.1X standartları ile gerçekler. 802.11i protokolü 2 katmandan oluşur: alt katmanda gelişmiş şifreleme algoritmaları (TKIP, CCNP) , üst katmanda ise kimlik asılama ve anahtar dağıtımı için 802.1X yer almaktadır. Veri bütünlüğü MIC ile sağlanır. Gezginlik sağlar. Gezginlik gerçek zamanlı iletişimlerde önem kazanır çünkü veri kaybını engeller. RSN gezginliği iki farklı şekilde gerçekler.

- Önceden asıllama: Öncende asıllamada kullanıcı bir erişim noktasına bağlı iken diğer bir erişim noktasının varlığının farkına varırsa 802.1x anahtar değişimi ile bu erişim noktası için de anahtarları elde eder ve saklar. Sinyal zayıflığı gibi nedenlerden önceden anahtarını elde ettiği AP'ye geçmek isterse 802.1x işlemlerini yapmaya kalmaz.
- Anahtar önbellekleme: Erişim noktası ile daha önceden anahtar belirlendi ise bu anahtarlar bellekte saklanır. Bu erişim noktası ile iletişime geçildiğinde 802.1x işlemlerini yapmaya kalmaz.

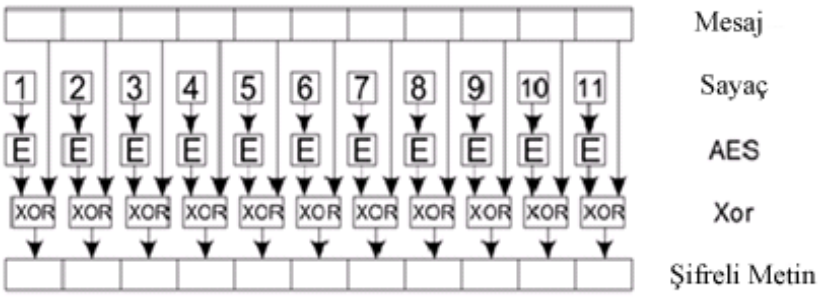
RSN de şifreleme Temporal Key Integrity Protocol (TKIP) veya Counter Mode with CBC-MAC Protocol (CCMP) ile gerçeklenir. CCMP zorunlu iken, TKIP ise seçeneklidir.

2.6.1 CCMP (Counter Mode –Cbc Mac Protocol)

CCMP içinde şifreleme algoritması AES(Advanced Encryption Standart) kullanır. AES güvenilir ve hızlı bir algoritmadır. Simetrik anahtar kullanır. CCMP içinde seçilen kullanım modu Counter Mode with CBC-MAC (CCM)dir. AES in birçok kullanım modu vardır. CCMP içinde olan kullanım modlarına bakacak olursak;

- Counter mode (gizlilik amaçlı) :

Sayaç yönteminin kullanılma amacı aynı veri içeren bloklar aynı şifre ile şifrelendiğinde farklı çıkışların olmasının istenmesidir. Çünkü mesajın tekrar eden bloklardan oluştuğunun bilinmesi bir zayıflıktır. Şekil 18 de Counter mode gösterilmiştir.



Şekil 2.29. AES counter (sayaç) çalışma modu [Matthew S.,2005]

Şekildende görüldüğü gibi veri blokları şifrelenmiş sayılar ile XOR işlemine tutulmaktadır. Burada kullanılan sayılar rasgele seçilmektedir çünkü aynı iki mesaj aynı çıkışları verecektir. Bu sayının başlangıcı karşı tarafa iletilmelidir. Bu AES 128 bitlik şifreleme anahtarı kullanılır.

- CBC- MAC modu (Bütünlük)

CBC-MAC modu ise MIC hesabında kullanılır. Eğer mesajda 1 bit değişirse MIC de büyük değişiklikler olur ve tahmin edilemez. MIC hesabı geri dönülmez bir şekilde yapıldığı için araya girenin mesaja uygun bir MIC hesaplaması mümkün değildir. Aşağıda MIC in hesaplanma yöntemi verilmiştir.

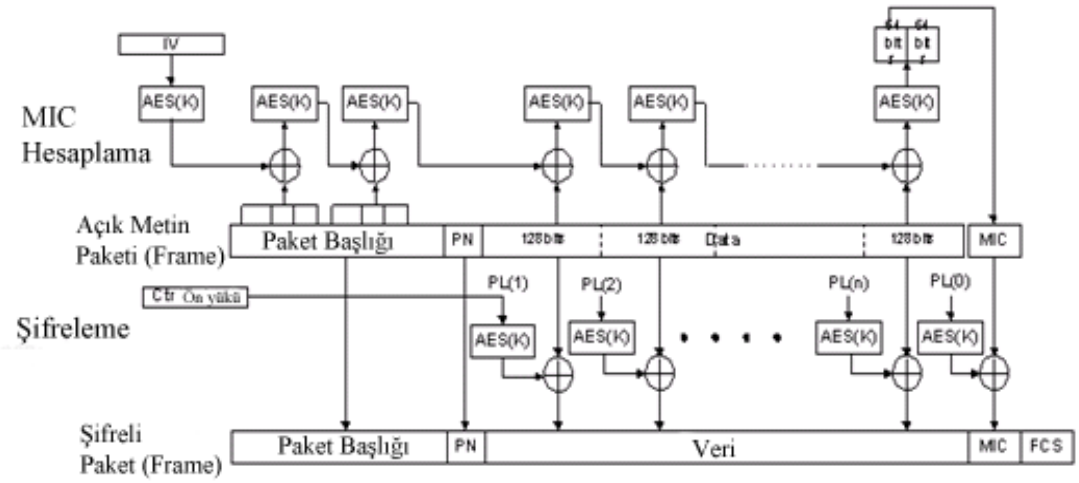
1) İlk veri bloğunu al ve AES i kullanarak şifrele.
2) Sonuç ile 2. Bloğu dar veya işlemine tut ve şifrele
3) Çıkan sonucu bir sonraki blok ile XOR işlemine tut ve şifrele

Şifreleme yöntemi adını bu iki modun birleşiminden almaktadır.

CBC- MAC + Counter mode = CCM

CCMP çalışma yapısına bakacak olursak öncelikle MIC hesabı için CBC-MAC(Cipher block chaninig message authentication code) kullanılır. Buradan oluşan 128 bitin 64 biti kullanılır.

Mesajın şifrelenmesinde de sayaçtan bir değer alınır ve AES algoritması ile şifrelenip daha sonra çıkan sonuç mesajın 128 lik ilk bloğu ile XOR işleminden geçer. Daha sonraki bloklarda sayaç birer arttırılarak elde edilen sayılar kullanılarak şifrelenir. Şekil 2.36'da CCMP çalışma biçimi gösterilmiştir.



Şekil 2.30. CCMP Çalışma Yapısı[Matthew S.,2005]

Bu protokol aşağıdaki sorunlara çözüm getirmiştir.

- Kimlik asıllama
- Şifreleme
- Yetkilendirme

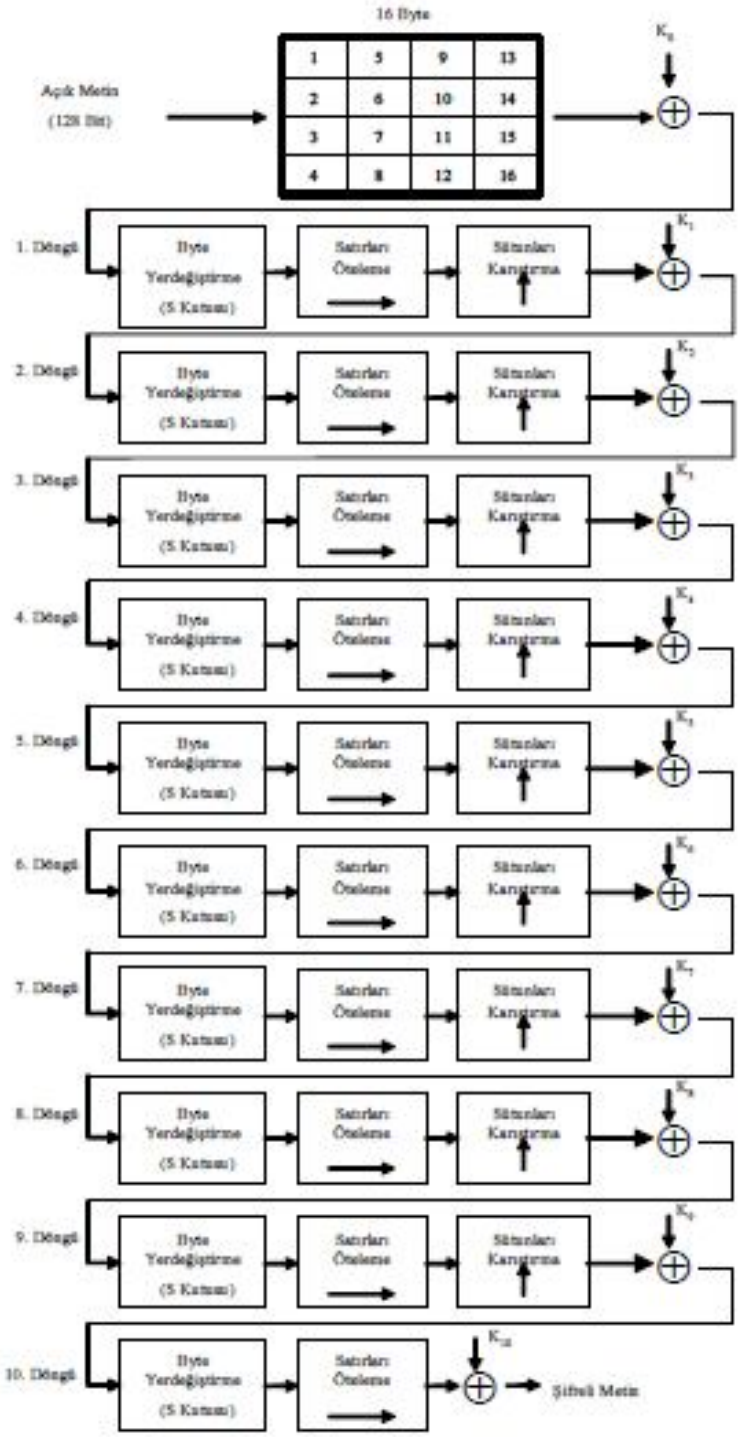
- Anahtar Yönetimi
- Korunmamış bilgilerin gönderilmesi / alınması
- Mesajın kaynağının asıllanması (taklidini önler)
- Mesajlara sıra numarası konması (replay saldırılarını önler)
- Her paket için şifreleme yapılmaması (Gereksiz şifrelemeyi engeller)
- Kaynak ve Varış adreslerinin korunması
- Gizlilik ve mesaj bütünlüğü için bir güçlü şifreleme algoritması kullanılması
- Qos gelişmelerine uyum sağlama yoluna gidilmiştir.

2.6.2 AES (Advanced Encryption Standard) Şifreleme Algoritması

AES (Rijndael) algoritması 128 bit veri bloklarını 128, 192, 256 bit anahtar seçenekleri ile şifreleyen bir algoritmadır. SPN algoritmasının geniş bir çeşididir. Döngü sayısı anahtar genişliğine göre değişmektedir. 128 bit anahtar için 10 döngüde şifreleme yaparken 192 ve 256 bit anahtarlar için sırasıyla 12 ve 14 döngüde şifreleme yapmaktadır[FIPS,2001].

AES algoritmasında her döngü dört katmandan oluşur. İlk olarak 128 bit veri 4×4 byte matrisine dönüştürülür. Daha sonra her döngüde sırasıyla byte'ların yerdeğiştirmesi, satırların ötelenmesi, sütunların karıştırılması ve anahtar planlamadan gelen o döngü için belirlenen anahtar ile XOR'lama işlemleri yapılır. Byte'ların yerdeğiştirilmesinde 16 byte değerinin her biri 8 bit girişli ve 8 bit çıkışlı S kutusuna sokulur. S kutusu değerleri, Galois cisminde (Galois Field - GF) $GF(2^8)$, 8 bitlik polinom için ters alındıktan sonra doğrusal bir dönüşüme sokularak elde edilmiştir. Satırların ötelenmesi işleminde 4×4 byte matrisinde satırlar ötelenmiş ve sütunların karıştırılması işleminde herhangi bir sütun için o sütundaki değerler karıştırılmıştır.

Döngünün son katmanında ise o döngüye ait anahtar ile XOR'lama yapılmaktadır. Şekil 2. 31. , 128 bit anahtar ile şifreleme için AES algoritmasını göstermektedir[Matsui,1994,Daemen J.,Rijmen V.,1998].



Şekil 2.31. Tüm AES Algoritması (128 bit anahtar için)

2.7 WEP, WPA ve WPA2 Karşılaştırması

Önceki bölümde Kablosuz yerel ağlarda kullanılan 3 şifreleme yöntemi incelenmiştir. Bunlardan WEP ve WPA-PSK günümüzde aircrack gibi üçüncü parti yazılımlar kullanılarak ortak anahtar elde edilebilir[Aircrack,2009]. Bunun için WPA kullanımı TKIP destekli kullanıldığında ve WPA2 şifreleme sistemi kullanıldığında daha etkili olmaktadır. Bu üç şifreleme sisteminin karşılaştırılması tablo 2.1'de gösterilmiştir.

	WEP	**WPA**	**WPA2**
Şifreleme	Şifreleme yapısı kırıldı. RC4 algoritması	WEP in açıklarını kapatıyor. TKIP/RC4	CCMP/AES CCMP/TKIP
Şifreleme Anahtarı	40 bitlik anahtar	128 bitlik anahtar	128 bit
IV	24 bit	48 bit	48 bit
Anahtar Değişikliği	Anahtar sabittir.	Anahtarlar her oturum, her paket için değişir.	Anahtar değişikliğine gerek yoktur.
Anahtar yönetimi	Anahtar yönetimi yoktur	802.1x	802.1x
Asıllama	Zayıf bir yöntem	802.1x EAP	802.1x EAP
Veri Bütünlüğü	ICV	MIC	MIC

Tablo 2. 1. WEP, WPA ve RSN Karşılaştırması

3. KABLOSUZ AĞLARA YAPILAN SALDIRI TÜRLERİ

Kablosuz Ağların kullanımı arttıkça kablosuz güvenlik konusu çok önem kazanmıştır. Saldırganlar standartlaşmış kablosuz güvenliği üzerinde açıklar aramakta ve çeşitli amaçlar doğrultusunda bazı yöntemler kullanarak saldırılar yapmaktadır. Bu saldırılar bazen basit zararlar getirse de, ticari kuruluş ve önemli iletişim devamlılığı gerektiren sistemler için büyük zararlar getirebildiği görülmüştür. Bu saldırıların temel amaçları gizli anahtarı ele geçirmek, kablosuz ağın iletişimini keserek diğer legal kullanıcıların iletimini sabote etmektir. IEEE,802.11i güvenli kablosuz ağ standardını oluştururken WEP gibi kablosuz ağlarda ilk zamanlarda kullanılan güvenlik standartlarının açıklarını gidererek, daha güvenli şifreleme algoritmaları geliştirmeye çalışmıştır. Kablosuz ağlardaki bu gelişim ve güvenlik, saldırganların saldırı yöntemlerine yönelik olmuştur. Fakat Martin Beck ve Erik Tews Kasım 2008'de WEP'ten sonra geliştirilen, TKIP kullanan WPA şifreleme sistemini kıran yöntemi geliştirerek kablosuz ağların bazı saldırı yöntemleri ile kablosuz güvenlikteki gelişmelere rağmen kırılabileceğini göster miştir. Bu Saldırı Yöntemleri literatürde yerini almıştır. Bu tezde, kablosuz ağlara yapılan atak çeşitleri, bu atakların amaçları itibariyle sınıflandırılması ve kullanılma sıklığına göre bir grafik elde edilmek istenmiştir.

3.1 Kablosuz Ağlara Yapılan Saldırıların Yöntem ve türüne Göre Sınıflandırılması

Kablosuz ağlara yönelik potansiyel tehdit ve kullanıldığında tesir edecek birden çok saldırı geliştirilmektedir. Bu yönde bu tezde 802.11 ve 802.1X 'e karşı yapılan atakların ya da tehditlerin bir referans listesi oluşturmak istenmiştir. Tehdit tiplerine göre kategori sağladık ve bu tehditleri yapan saldırganların metotlarını ve kullandıkları araçlar gösterilmiştir.

Tehdit türleri aşağıdaki şekilde sınıflandırılabilir;

a) Erişim Kontrolü Saldırıları (Access Control Attacks)
b) Gizlilik Saldırıları (Confidentiality Attacks)
c) Bütünlük Doğrulama Saldırıları(Integrity Attacks)
d) Kimlik Doğrulama Saldırıları (Authentication Attacks)
e) Kullanılabilirlik saldırıları (Availability Attacks)

3.1.1 Erişim Kontrolü Saldırıları (Access Control Attacks)

Bu saldırılar, Erişim Noktası MAC filtrelemesi ve 802.1X port erişim kontrolü gibi Kablosuz Ağ erişim kontrol önlemlerine karşı, radyo frekanslarını gizlice dinleyerek ağ girmeyi dener. Kısaca Kablosuz Ağda bulunan Erişim kontrol önlemlerini anlayarak bunları delip sisteme girmek için yapılan ataklardır (Tablo 3.1).

Saldırı Tipi	Özet Açıklama	Methodlar ve Araçlar
War Driving	Araştırma isteklerini ya da beacon denilen istemcilerin dinlemeye geçmesi için gönderilen iletileri dinleyerek Kablosuz bir Ağ keşfetmektir. Bu sebeple diğer saldırılar için bir uç sağlamaktır.	Airmon-ng, DStumbler, KisMAC, MacStumbler, NetStumbler, Wellenreiter, WiFiFoFum
Rogue Access Points	Güvenli bir ağ içinde bir arka kapı yaratmak için, güvenlik duvarının iç tarafında bir güvensiz Erişim Noktası kurulmasıdır.	Her hangi bir donanım ya da yazılım Erişim Noktası (Access point) olabilir.
AdHoc Associations	Saldırı istasyonu ya da Erişim Noktası güvenliğini engellemek için doğrudan güvenli olamayan istasyona bağlanmak.	Herhangi bir kablosuz ağ kartı veya USB adaptör.
MAC Spoofing	Güvenli bir Erişim noktası veya istasyon süsü vererek saldırganın MAC adresini tekrar konfigure etmesidir.	MacChanger, SirMACsAlot, SMAC, Wellenreiter, wicontrol, NIC MAC, MAC MakeUp,
802.1X RADIUS Cracking	Şeytan İkizi Erişim Noktası(Evil twin AP)'nın kullanması için kaba kuvvet (kaba kuvvet) yoluyla 802.1X erişim isteklerinden RADIUS gizlilerini elde etmek.	Yerel alan ağları (LAN) ya da Erişim noktası ile RADIUS Server arasındaki ağ yolu üzerinde veri paketlerini toplama aracı.

Tablo 3.1. Erişim kontrolü saldırı çeşitleri [Lisa P.,2009]

3.1.1.1 Kablosuz Ağları Tarama (War Driving)

Wardriving, ilk ve en çok bilinen kablosuz ağ tespit etme (tabii ki güvenliği olmayan ya da az olan) metodudur. Genellikle bir gezici birim ile mesela dizüstü veya el bilgisayarları ile kullanılır. Wardriving taraması son derece ustalıkla ve çok basit yollarla gerçekleşir: Saldırgan dizüstü veya el bilgisayarı ile arabasında otururken bir kablosuz ağ tespit edebilir. Bir kere uygun bir AP tespit edildikten sonra saldırgan bunu kullanılabilir klasör olarak tanımlar ve araştırabilir. Ve hatta internete ulaşmasını engelleyebilir. Wardriving için kullanılan 'war' kelimesi aslında eski zamanlarda kullanılan Wardialing'den gelmektedir. Wardialing, saldırı amacıyla kullanmak üzere bir telefon numarasının bütün ihtimallerini deneyerek modem takılı olan hattı bulmak olarak tanımlanabilir. Bu yazıda kullanılan Wardriving de kablosuz ağlar için aynı mantıkta kullanılmaktadır.

3.1.1.2 Yetkisiz Erişim Noktası (Rogue Access Point)

Bir yetkisiz erişim noktası, hassas bilgilere erişmek isteyen kötü niyetli kişilerin kullandığı ya da yeterince güvenlik bilgisi olmayan yöneticilerin kendi veya şirket faydası için ofislerine kurdukları AP'lerdir. Her iki durumda da, bu yetkisiz AP'ler güvenliği tehdit etmektedir.

Yetkisiz AP'ler, karışmaya (interference) neden olacaklar ve sistem başarımını düşüreceklerdir. Daha da kötüsü, yetkisiz kişilerin (saldırgan) ağa erişmesine neden olmaktadır. Telsiz ağ durakları, ilişkilendirildikleri AP'den ayrılıp, kendilerine daha yakın olana bir yetkisiz AP ile ilişkilenebilirler. Bu durum WEP'in etkin duruma getirilmemesinde oluşur. Yetkisiz AP'den faydalanan bir saldırgan, yetkisiz AP ile ilişkilenen diğer ağ duraklarına erişebilir. Yetkisiz AP'nin kablolu ağ tarafına da bağlı olması, saldırganların kablolu ağa da erişmesini sağlamaktadır.

3.1.1.3 Mac Adres Sahteciliği (Mac Spoofing)

Güçlü kimlik formları kullanıldığında ALC (Erişim Kontrol Listeleri) ler kabul edilebilir bir güvenlik seviyesi sağlamaktadırlar. Ne yazık ki ayni şey MAC adresleri için geçerli değildir. MAC adresleri WEB kullanılabilir durumda iken dahi şifresiz metin olarak saldırgan tarafından kolaylıkla dinlenebilir. Ayrıca, kablosuz ağ kartlarının bir yazılım vasıtası ile MAC adresleri kolaylıkla değiştirilebilir. Saldırgan tüm bu avantajları kullanarak ağa nüfuz edebilmektedir.

MAC adresini dinlemek çok kolaydır. Paket yakalama yazılımı kullanarak saldırgan kullanılan bir MAC adresini tespit eder. Eğer kullandığı kablosuz ağ kartını izin veriyorsa MAC adresini bulduğu yeni MAC adresine değiştirebilir ve artik hazırdır. Eğer saldırgan yanında kablosuz ağ donanımı bulunduruyorsa ve yakınında bir kablosuz ağ varsa, artik aldatma saldırısı yapabilir demektir. Aldatma saldırısı yapabilmek için, saldırgan kendine ait olan AP'yi yakınındaki kablosuz ağa göre veya güvenebileceği bir internet çıkısı olduğuna inanan bir kurbana göre ayarlamalıdır. Bu sahte AP'nin sinyalleri gerçek AP den daha güçlüdür. Böylece kurban bu sahte AP'yi seçecektir. Kurban bir kere iletişime başladıktan sonra, saldırgan onun şifre, ağ erişim ve diğer önemli bütün bilgilerini çalacaktır. Bu saldırının genel amacı aslında şifre yakalamak içindir. Bunu yapmanın birkaç yolu vardır. Kendimiz adres değişikliği yapabiliriz. Ağ üzerinde bir Ethernet frame gönderdiğimizde yazılım vasıtasıyla bu alana müdahale edip, tekrardan configüre edebiliriz. Bazı kartlar Windows'taki denetim ayarları vasıtasıyla MAC adreslerini düzenlemeye yardımcı olur. Kart içerisindeki adresi yenileyebiliriz. Bunun için kullanılan chipset'in özelliklerini bilen bir yazılıma ihtiyaç duyup, kart üzerine yeni bir adres atanması sağlanabilir. Anakart üzerindeki dâhili ethernet kartlarının MAC adresleri de BIOS ayarlarından değiştirilebilir. Linux kullanıcıları aldatma yazılımı olmaksızın "ifconfig" gibi tek bir parametre kullanarak MAC adreslerini değiştirebilir. Aynı zamanda Mac adres değiştiren birçok program internette mevcuttur[Wright J.,2003].

3.1.1.4. Ip Adresi Yanıltma (Ip Spoofing)

İnternetin çalışmasını sağlayan TCP/IP [http://www.networkmagazine.com] protokol ailesi geliştirilirken güvenlik temel amaç olmadığı için olabildiğince esnek davranılmıştır. Bu esneklik IP adreslerinin aldatılabilir (spoofed) olmasını sağlamıştır. Ip spoofing yaparak başkasının IP adresinden istenilen internet aktivitesi yapılabilir. Son yazdığımız cümle bundan on sene öncesi için geçerli olsa da günümüzde pratik olarak geçersizdir. Bunun temel nedeni günümüz modern işletim sistemlerinin protokoldeki eksik noktalara kalıcı çözüm getirmeleridir. Özellikle internet de en sık kullanılan HTTP, SMTP, HTTPS gibi protokollerin temelinde bulunan TCP bu tip sahtecilik işlemlerini engelleme amaçlı bir yöntem kullanır[Rahman L., Zhou R. ,2003].

3.1.1.5 Güvenli Olmayan Ağa Bağlanma (Adhoc Associations)

Araçların direk olarak birbirleriyle iletişimine imkân sağlar. Araçlar ağ içerisinde hareket edebilir ve kendi kapsama alanında olan herhangi bir araca bağlanabilir. Baz istasyonu yoktur. Düğümler sadece kapsama alanındaki diğer düğümler ile haberleşir. Düğümler ağ içinde kendilerini organize eder.

3.1.1.6 802.1x Radius Cracking

Şeytan İkizi Erişim Noktası(Evil twin AP)'nın kullanması için kaba kuvvet (brute force) yoluyla 802.1x erişim isteklerinden RADIUS gizlilerini elde etme yöntemidir. Bir başka deyişle bu saldırıyı yapacak saldırgan, yerel alan ağları ya da erişim noktası ile RADIUS Server arasındaki ağ yolu üzerinde veri paketlerini toplamak için uğraşır.

3.1.2 Gizlilik Saldırıları (Confidentiality Attacks)

İster Yüksek katman protokolleri olsun, ister 802. 11 içinde şifreli ya da açık gönderimler olsun, Bu ataklar kablosuz bağlantılar üzerinden gönderilen özel bilgileri engellemek için girişimde bulunurlar (Tablo 3.2).

Saldırı Tipi	Özet Açıklama	Methodlar ve Araçlar
Eavesdropping	Yakalanmış ve şifresi çözülmüş korumasız uygulama trafiği içinde olanak dâhilinde hassas bilgiyi ele geçirir. Gizlice dinleme anlamına da gelir.	bsd-airtools, Ettercap, Kismet, Wireshark, commercial analyzers
WEP Key Cracking	Kaydedilmiş veri, aktif ya da pasif Methodlar kullanarak bir WEP anahtarı elde eder.	Aircrack-ng, airoway, AirSnort, chopchop, dwepcrack, WepAttack, WepDecrypt, WepLab, wesside
Evil Twin AP	Yem ya da legal kullanıcılara WLAN'ın servis seti Tanımlayıcısını (SSID) hat kesinti iletisi yoluyla yetkili bir Erişim noktası gibi göstermesidir.	cqureAP, D-Link G200, HermesAP, Rogue Squadron, WifiBSD
AP Phishing	Kredi kartı numaralarını, kullanıcı giriş şifrelerini çalmak için Şeytan İkizi Erişim Noktası(Evil Twin AP) üzerinde Web Server ya da sahte bir portal çalıştırmak.	Airpwn, Airsnarf, Hotspotter, Karma, RGlueAP
Man in the Middle	TCP oturumlarını(sessions) veya SSL/SSH tünellerini(tunnels) kesmek için Şeytan İkizi Erişim Noktası(Evil Twin AP) üzerinde geleneksel ortadaki adam saldırı (Man in the Middle) araçlarını çalıştırmak.	dsniff, Ettercap-NG, sshmitm

Tablo 3. 2. Gizlilik Saldırıları (Confidentiality Attacks) [Lisa P.,2009]

3.1.2.1 Gizli Dinleme (Eavesdropping)

Bir ağ veya kanal üzerinden iletilen verinin, kötü niyetli üçüncü kişiler tarafından araya girilerek alınmasıdır. Bu saldırı tipinde, hatta kaynaktan hedefe giden verinin arada elde edilip, değiştirilerek hedefe gönderilmesi bile mümkündür. İngilizce "eavesdropping" (saçak damlası) olarak adlandırılan bu saldırının, sanıldığının aksine

çok farklı uygulama alanı bulunmaktadır. Hiç bir bilgisayarla etkileşimi olmayan tek başına çalışan bir bilgisayar bile, mikroçip, ekran veya yazıcı gibi elektronik parçalarından yayılan elektrik veya elektromanyetik yayılım takip edilerek gizlice dinlenebilir. Bu cihazların bu tür dinlemelere olanak vermemesi için, Amerikan hükümeti 1950'li yılların ortasından başlayarak TEMPEST adında bir standart geliştirmiştir.

3.1.2.2 Wep Anahtarı Kırma (Wep Key Cracking)

WEP'in açıkları ile alakalı birden çok makale yayınlanmıştır. Wep'in zayıflıkları yüzünden günümüzde gelişmiş WPA, WPA-2 gibi daha güvenli standartlar oluşturulmuştur. Wep'in bu açıkları saldırganları aktif ya da pasif saldırılar düzenlenmesine olanak sağlar. Amaç WEP anahtarını kırılmasıdır. Frekans bandı dinlenerek sonuca varılmaya çalışılır. Pasif Saldırılar IV çakışmalarından elde edilen sonuçlara göre yapılan saldırılar olup, aktif saldırılar ise Replay (tekrar) saldırıları ve mesajın içeriğini değiştirerek yapılan saldırılardır.

3.1.2.3 Şeytan İkizi Erişim Noktası (Evil Twin Ap)

Saldırganlar, söz konusu sistemi şaşırtmak için, kullanılmakta olan Access Point'un benzerini yaratıp, kullanıcıların o, Erişim noktasını kullanmasını sağlayabilirler. Böylelikle, yaratılmış ikiz AP ye giren kullanıcının tüm bilgileri elde edilebilir.

3.1.2.4 Ap Üzerinde Sahte Portal Çalıştırmak (Ap Phishing)

Saldırganlar kullanıcıların Evil Twin AP'ye bağlanmasından sonra bir Web sunucusu kurarak, bu saldırganları çeşitli web sayfalarına yönlendirip, hedefi olduğu kişiler hakkında, sayfadaki zararlı kodlar vasıtasıyla bilgi toplayabilirler.

3.1.2.5 Ortadaki Adam Saldırısı (Man In The Middle)

Bu saldırı yöntemine bu alanda farklı kaynaklarda bucket brigade attack (elden ele kova saldırısı) ismi de verilir. Buradaki benzetme eski zamanlarda itfaiye erlerinin elden ele taşıdıkları ve yangını söndürmek için kullandıklara kovalardan gelmektedir. Bu saldırıda, saldırgan hedef iki bilgisayar arasındaki iletişimi ele geçirmek üzere kendini araya ekler. Verilerin iki hedef arasında doğrudan iletilmesi yerine, saldırgan üzerinde değişime uğratılarak gönderilir. Fakat bu işlemi iki bilgisayarda anlayamaz.

1.) Kablosuz saldırgan, kablolu ağdaki anahtara takılı AP üzerinden aynı anahtara takılı olan 2 ayrı kullanıcıya ortadaki adam saldırısını gerçekleştirebilir.

2.) Kablosuz saldırgan, kablosuz bir kullanıcı üzerinden, AP nin takılı olduğu hub veya anahtara ortadaki adam saldırısı yapabilir.

3.) Kablosuz saldırgan farklı AP lerde olan kullanıcılara her iki AP'yi de kapsayan bir saldırı düzenleyebilir

3.1.3 Bütünlük Doğrulama Saldırıları (Integrity Attacks)

Diğer atak tiplerini kolaylaştırmak ve ya alıcıyı yanıltmak için bu ataklar, sahte kontrol, yönetim ve ya kablosuz iletişim üzerinden veri paketleri gönderir (Tablo 3.3). DoS saldırıları buna örnektir. DoS saldırıları ayrı bir bölüm olarak incelenmiştir.

3.1.3.1 802.11 Paketi Püskürtme (Frame Injection)

Bu yöntem, sahte 802.11 paketlerini erişim noktalarına ya da saldırgana göndererek, bir süre sonra kaynağın ya servis dışı olmasına ya da gerekli bilgileri dışarı vermesini sağlar. Bunun çok çeşitli programlar vardır. Bu programlar için ya da başka deyişle püskürtme için önemli olan programlar şu mantığı uygular.

Saldırı Tipi	Özet Açıklama	Methodlar ve Araçlar
802.11 Frame Injection	Sahte 802. 11 paketlerini(frames) göndermek.	Airpwn, File2air, libradiate, void11, WEPWedgie, wnet dinject/reinject
802.11 Data Replay	Daha sonra tekrar için 802. 11 veri paketlerini(frames) yakalamak.	Capture + Injection Tools
802.1X EAP Replay	Daha sonra tekrar için 802.1X Genişletilebilir Kimlik doğrulama protokolleri yakalama(Extensible Authentication Protocols) (v.s. EAP kimlik, başarı, Hata)	Wireless Capture + Injection Tools between station and AP
802.1X RADIUS Replay	Daha sonra tekrar için RADIUS Erişim Kabul ve ya Ret mesajlarını yakalamak.	Ethernet Capture + Injection Tools between AP and authentication server

Tablo 3. 3. Bütünlük Doğrulama Saldırıları (Integrity Attacks) [Lisa P.,2009]

a) İlk önce Erişim noktası araştırılır.
b) Açıklar aranır.
c) De-Authentication ve De-association saldırıları için paket püskürtürler.
d) Her donanım sürücüsünü desteklemedir.

3.1.3.2 802.11 Veri Tekrarlama (802.11 Data Replay)

Bir saldırı tekrarı için hem paket toplamak, hemde aynı zamanda bu paketleri yineleyerek püskürtmek amaçlıdır. İşin içinde hem kayıt etmek hem de paket püskürtme tekrarları vardır.

3.1.3.3 802.1x EAP Tekrarlama (802.1x EAP Replay)

802.1X Genişletilebilir Kimlik doğrulama protokollerinden paket yakalamak amaçlıdır. Böylece sisteme bu paketlerle tekrar saldırısı yapabilir.(Extensible Authentication Protocols) (v.s. EAP kimlik, başarı, Hata gibi paketleri yakalar)

3.1.3.4 802.1x Radius Tekrarlama (802.1x Radius Replay)

RADIUS Erişim Kabul ve ya Ret mesajlarını yakalamaktır. Erişim noktası ile Kimlik doğrulama ana makinesi arasında tekrar saldırıları yapmakta sonra gelen adımdır.

3.1.4 Kimlik Doğrulama Atakları (Authentication Attacks)

Davetsiz misafirler bu atakları, legal kullanıcıların kimlik ve kimlik bilgilerini çalarak özel bir ağa veya servise bağlanmak için kullanırlar (Tablo 3.4).

Saldırı Tipi	Özet Açıklama	Methodlar ve Araçlar
Shared Key Guessing	Kırılmış WEP anahtarı ya da varsayılan sağlayıcı ile 802. 11 paylaşımlı anahtar kimlik doğrulayıcısını tahmin etme girişiminde bulunmak.	WEP Cracking Tools
PSK Cracking	Sözlük Saldırı araçları kullanarak kaydedilmiş anahtar tokalaşma (handshake) paketlerinden WPA/WPA2 PSK'yı elde etmek.	coWPAtty, genpmk, KisMAC, wpa_crack
Application Login Theft	Açık Metin uygulama protokollerinden kullanıcı bilgilerini yakalama.(e-mail, adres, şifre)	Ace Password Sniffer, Dsniff, PHoss, WinSniffer
Domain Login Cracking	Sözlük veya kaba kuvvet saldırıları kullanan karma NETBIOS şifre kırma işlemi yoluyla kullanıcı bilgilerini (Windows Giriş ve şifre) elde etmek.	John the Ripper, L0phtCrack, Cain
VPN Login Cracking	VPN kimlik doğrulama protokolleri üzerinde kaba kuvvet saldırıları kullanarak kullanıcı kimlik bilgilerini(PPTP şifresi veya IPsec Preshared Secret Key) elde etmek.	ike_scan and ike_crack (IPsec), anger and THC-pptp-bruter (PPTP)
802.1X Identity Theft	Açık metin 802.1X Kimlik yanıtlama paketlerinden kimlik bilgilerini yakalamak.	Capture Tools
802.1X Password Guessing	Yakalanan bir kimliği kullanarak, 802.1X kimlik doğrulama yönteminde kullanıcın şifresini tahmin etmek için ardı ardına girişimde bulunmak.	Password Dictionary
802.1X LEAP Cracking	NT şifre karmalarını kırmak için sözlük saldırı araçları kullanarak kayıt edilmiş EAP(LEAP) zayıf 802.1X paketlerinden kimlik bilgilerini elde etmek.	Anwrap, Asleap, THC-LEAP cracker
802.1X EAP Downgrade	Sahte EAP-Response/Nak paketleri kullanarak 802.1X Serverı bir zayıf kimlik doğrulama tipine istekte bulunmaya zorlar.	File2air, libradiate

Tablo 3. 4. Kimlik Doğrulama Atakları (Authentication Attacks) [Lisa P.,2009]

3.1.5 Kullanılabilirlik Saldırıları (Availability Attacks)

Bu ataklar, yasal kullanıcılara yönelik kablosuz servislerin verimini azaltmak ve ya engellemek için kullanılır. Amaç, gerek bu kullanıcıların WLAN kaynaklarına erişimini engellemek gerekse de kaynaklarını azaltmaya yöneliktir (Tablo 3.4).

Saldırı Tipi	Özet Açıklama	Methodlar ve Araçlar
AP Theft	Kullanım uzayından fiziksel olarak erişim noktasını çıkarmak.	"Five finger discount"
Queensland DoS	Meşgul görünen bir kanal yapmak için CSMA/CA'dan yararlanmak.	An adapter that supports CW Tx mode, with a low-level utility to invoke continuous transmit
802.11 Beacon Flood	İstasyonların yasal bir Erişim noktasını bulmasını zorlaştırmak için binlerce sahte 802. 11 beacon(hat kesme iletisi) üretmek.	FakeAP
802.11 Associate / Authenticate Flood	Bir erişim noktasının dâhil olma (association) tablosunu doldurmak için rastgele MAC adreslerinden sahte kimlik doğrulama ve dâhil olmalar göndermek.	FATA-Jack, Macfld
802.11 TKIP MIC Exploit	Geçersiz TKIP verileri üreterek, Erişim noktasının MIC hata eşiğini aşmasını, WLAN servislerinin askıya alınmasını sağlar.	File2air, wnet dinject, LORCON
802.11 Deauthenticate Flood	Erişim noktasından, bağlı olmayan kullanıcıları istasyonlar aracılığıyla sahte kimlik doğrulamama ve dâhil olmama mesajlarına boğmak.	Aireplay, Airforge, MDK, void11,commercial WIPS
802.1X EAP-Start Flood	Hedefi çökertmek ya da kaynakları tüketmek için EAP-Start mesajları aracılığıyla Erişim Noktasını boğmak.	QACafe, File2air, libradiate
802.1X EAP-Failure	Geçerli bir 802.1X EAP değişimini gözlemledikten sonra istasyona sahte EAP-Hata mesajları göndermek.	QACafe, File2air, libradiate
802.1X EAP-of-Death	Hatalı oluşturulmuş 802.1X EAP Kimlik yanıtı göndererek bilinen bir Erişim noktasını çökmeye çalışır.	QACafe, File2air, libradiate
802.1X EAP Length Attacks	Kötü uzun alanlar aracılığıyla EAP özel tip mesajlar göndererek bir Erişim noktası ve ya RADIUS sunucuyu çökertmeye çalışmayı denemek.	QACafe, File2air, libradiate

Tablo 3. 5. Kullanılabilirlik Saldırıları (Availability Attacks) [Lisa P.,2009]

3.1.6 Servis Reddi Saldırıları (DoS Attacks)

DoS atakları karşı sistemde çalışan servisin durdurulması veya çalışmasının aksatılmasını hedefleyen saldırı tipidir. Saldırgan istemci diğer legal istemcilerin bilgi erişimini ya da servisleri erişimini engellemeye çalışır. Bu tip saldırılarda şifre kırılması

ya da bilgi çalınması gibi olaylar amaç değildir. Bu saldırılar iki şekilde servisi durdurmaya çalışırlar:

- İşlemci, hafıza, bant genişliği gibi kavramları tüketerek
- Protokol ya da serviste bulunan bir zayıflığı kullanarak

DoS teknik olarak şöyle çalışır: Saldırının çalıştığı bilgisayar bir web site ya da sunucuya istek gönderir, sunucu bu isteğe cevap verir, saldırgan bu istekleri devamlı göndererek sunucuya yük bindirir ve sunucu işlem yapamaz hale gelir. Kaynaklarını tüketir. Bunun sonucu olarak diğer kullanıcılar da web sitesi ya da erişim noktasına erişemez duruma gelirler. Bunun yanı sıra DoS atakları Spam E-mail mesajlarda kullanarak kotaları şişirip diğer mesajların gelmesini engelleyebilir

DoS atak belirtileri:

- Alışık olunmayan düşük ağ performansı
- Bir web sitesine erişmede yavaşlık
- E-Mail kutusunda ki Spam E-Maillerinin artışı
- Web sitelerinin belirli bölümlerinin kullanılamaması

DoS ataklarının birçok türü ve tekniği bulunmaktadır. Günümüzde çoğu firma DoS ataklarını engellemek ve anlamak açısından yazılımlar ya da donanımlar üretmişlerdir. Fakat DoS atakları günümüzde hala bazı güvenlik zafiyeti olan erişim cihazı ya da web sitesi üzerinde etkili olmaktadır [Gezgin ve Buluş, 2007].

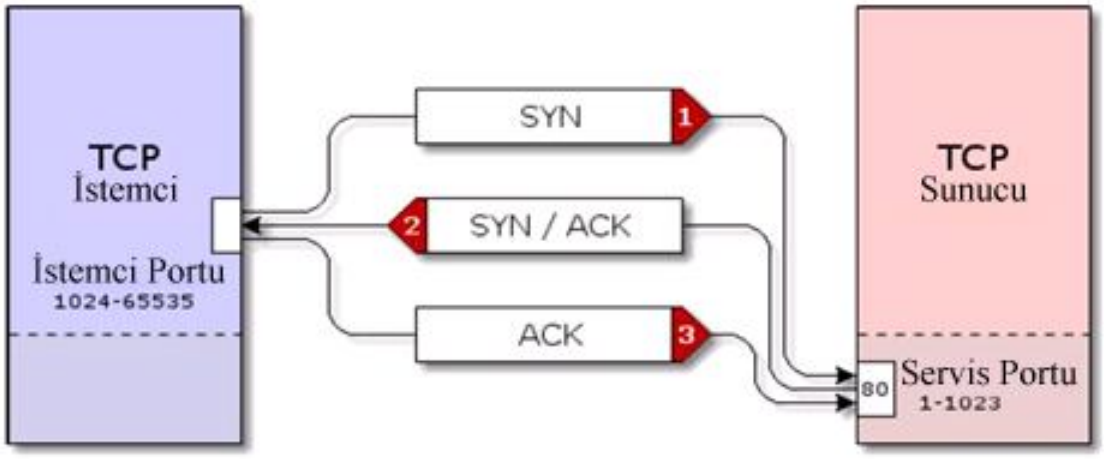
3.1.6.1 DoS Atak Türleri

- TCP/SYN Flood Attack:

Bu atak türü klasik bir DoS saldırısıdır ve modern ticari bilgisayar sistemlerinde bu saldırılara karşı önlemler alındığından fazla etkili değildirler. Bu saldırı tekniğine göre hedef sisteme gelen SYN (Synchronize) paketleri hedef sistemin hafızasını doldurur. Hafızası dolan sunucu diğer sisteme bağlı istemcilere servis veremez duruma

gelir. İlk olarak istemci ile sunucu arasında bir bağlantı nasıl hangi adımlardan bunu görelim. Bu olay 3 adımdan oluşur

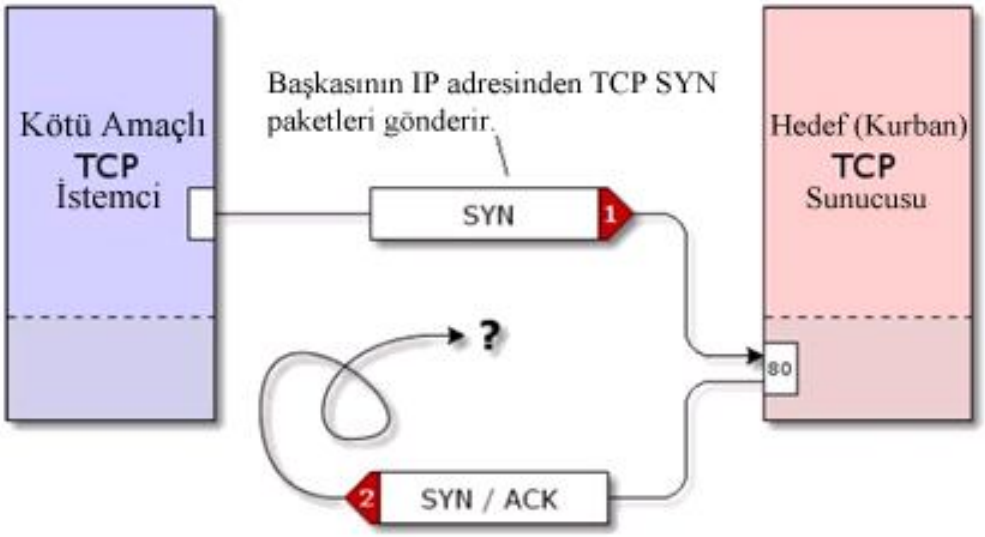
1. İstemci, sunucu makineye bağlanmak için kendisi hakkında bilgi bulunan bir SYN paketi yollar.(Web, Telnet, Mail, FTP gibi)
2. Sunucu bu SYN paketini alır ve bu paketi aldığını gösteren ACK (AcKnowledgement) ile SYN paketini birleştirerek istemciye gönderir. (ACK+SYN)
3. İstemci, sunucudan gelen bu paketleri alır ve aldığını gösteren bir ACK paketi yollar. Böylece bağlantı başlamış olur.



Şekil 3. 1. TCP 3 Aşamalı Tokalaşma

[TCP Tokalaşması, 2002**]**

Yukarıda anlatılan normal bir bağlantıdır. İşin saldırı kısmına baktığımızda 3. Adımda istemcinin sunucuya göndereceği ACK paketi sunucuya gönderilmediği takdirde sunucu istemciden ACK paketini beklemeye başlar ve bir süre bekler. Bu bekleme anında istemci tekrar bir bağlantı isteği oluşturup her defasında 3.Adımda ki ACK paketini sunucuya göndermezse her bağlantı için sunucu bu istekleri hafızasına kaydeder. Böyle ardı ardına işlem yapıldığında artık istemcinin hafızasını isteklerle doldurmuş oluruz. Bu sunucunun hafızası dolduğunda diğer kullanıcılara artık sunucu cevap veremez olur. Bu bize bir TCP/SYN Flood Attack yapıldığını gösterir.



Şekil 3. 2. TCP SYN Saldırısı

[TCP Tokalaşması,2002**]**

- TCP Replay Flood Attack

Bir kablosuz erişim noktasına açık olduğu portlardan yüksek miktarda veri göndererek hafızayı şişirmeyi sağlamaktır. Bu teknikte MAC Spoofing veya IP Spoofing gibi yöntemlerde beraber kullanılarak saldırının şiddeti arttırılır.

- Land Attack

Land attack aynı kaynak ve hedef yani kurbanın IPlerini ve portlarını sahte IP olarak içeren spoofed paketler gönderilmesi mantığı ile çalışan DoS saldırı türüdür. Bu paket el-sıkışma süreci ile sonuçlanan bir bağlantı talebi içerir. El-sıkışma sürecinin sonunda kurban bir ACK yani onay isteği gönderir. Hedef ve kaynak koordinatları aynı olduğundan kurban kendi gönderdiği istek paketini alır. Alınan veri kurbanın beklediği tür ile uyuşmaz, bu yüzden ACK isteği tekrar gönderilir. Bu süreç ağ çökene kadar devam eder.

Bu atak çeşidinde saldırganlar (hacker) hedef sistemin IP adresini, kaynak IP adresi olarak kullanarak ağı SYN paketleri ile istila ederler. Bu durumda host bilgisayar sanki paketleri kendi kendine göndermiş gibi görünür. Bu durumda hedef sistem kendi kendine yanıt vermeye çalışırken sistem kullanılamaz duruma gelir.

- *Brute-Force Attack*

Brute-force attack, örneğin 'Smurf' atağı, Bu tip ataklar bilgisayar ağını gereksiz verilerle istila ederler. İstila için IP tanımlamasındaki directed veya subnet broadcasting özelliğini kullanırlar. Bu atağı kullanan saldırgan, paketlerin hedef adresini networkün broadcast adresi olarak seçer. Bu durumda router networkteki bütün host'lara ICMP echo isteği gönderecektir. Eğer networkte aşırı derecede host varsa, bu büyük miktarda ICMP echo istek paketi oluşturacaktır. Broadcast seli mevcut band genişliğini tüketecektir. Bu durumda haberleşme mümkün olmayacaktır.

- *IP Spoofing Attack*

Ip Spoofing, sistemlere girmek için, saldırganın kimliğini gizleyebilmesi için veya DoS atağının etkisini büyütmek için kullanılır. IP Spoofing yönlendiriciyi veya güvenlik duvarını kandırarak isteğin güvenilir ağdan geldiğini sağlamaya çalışan bir tekniktir. Bu sayede sistemlere yetkisiz erişim sağlanır. Saldırgan bunu yapmak için paketin başlığını değiştirir. Bu sayede paket güvenilir ağdan geliyormuş gibi gözükür ve yönlendirici veya firewall bu paketlere izin geçişine izin verir.

- *Ping Flood Attack*

Ping Flood temel bir DoS atak türüdür. Bu tekniğe göre saldırganlar kurban sistemlere büyük boyutta (65000) ICMP paketleri göndererek sistemin bant genişliğini doldururlar. Böylece ağ iletişimini sabote ederler. Buna örnek Ping of Death atağıdır. Ping of Death atağı "PING" uygulamasını kullanarak IP tanımlamasında izin verilen 65535 byte veri sınırını aşan IP paketleri oluşturur. Normalden büyük paket daha sonra ağa gönderilir. Sistemler çökebilir, durabilir veya kapanıp açılabilir.

- *Teardrop Attack*

Teardrop atağı IP paketlerinin tekrar birleştirilmesindeki zayıflığı istismar eder. Veri, ağlar içinden iletilirken genellikle daha küçük parçalar ayrılır. Her bir parça orijinal paket gibi görünür. Ama istisna olarak offset alanı vardır. Teardrop programı bir

dizi IP paket parçaları oluşturur. Bu parçalar örtüşen offset alanlarına sahiptir. Bu parçacıklar varış noktasında tekrar birleştirildiklerinde bazı sistemler çökebilir, durabilir veya kapanıp açılabilir.

- *UDP Flood Attack*

Hızlı, ancak güvensiz bir iletişim protokolüdür. Gönderici bilgisayar veriyi gönderir ancak verinin ulaşıp ulaşmadığını kontrol etmez. Hızın önemli olduğu durumlarda tercih edilir. Bu atak tipi bilgisayar ağ protokollerinden UDP (User Datagram Protocol)'yi kullanan DoS ataktır. DoS atak için UDP' yi kullanmak TCP gibi kolay ve açık değildir. Aksine UDP Flood Attack uzaktaki erişim noktası üzerinde ki rastgele portlara büyük değerli UDP paketleri göndererek atak yapabilir. Genel mantığı sahte olarak üretilen IP adreslerinden paket yollamaktır. IP Spoofing kullanımı mecburi denilebilir. Örneğin bir bilgisayar flood(taşma) yapıyorsanız verinin doğru gidip gitmediğinden çok verinin çabuk gidip gitmediğini hesaplarsınız.

3.1.7 Dağıtık Servis Reddi Saldırıları (Distributed DoS Attack)

DDoS, trojan gibi yazılımlarla birçok sistemin hedefe saldırı yapmasını sağlamaktır. Bu sistemlere zombie adı verilir. Network bant genişliğini ve hedefin kaynaklarını bitirmek DDOS saldırısının amaçlarındandır diyebiliriz. DDOS saldırısının özellikleri:

- DDOS saldırısı birçok farklı IP adresinden geldiği için engellenmesi ve tespit edilmesi oldukça zordur. Fakat tek bir sistemden yani tek bir IP adresinden yapılmış olan saldırılar engellenebilir.
- Bu saldırı türünde hedefin servisleri asıl kurbandır. Farkında olmadan saldırı yapan ele geçirilmiş zombie sistemler 2. kurbandır.
- Hedefin servislerine yapılan geniş açılı ve koordineli saldırıdır.

4. KABLOSUZ AĞLARA YAPILAN SALDIRI (ATAK) UYGULAMALARI

4.1 Wep Şifrelemesinin Aircrack Programı İle Kırılması

Bu uygulamamız için işletim sistemi olarak Linux türevi ve en popüler olan Ubuntu LTS 10.0.3 kullanılmıştır. Şifre kırma programı olarak aircrack-ng 1. 0 programı kullanılmıştır. Şifre kırma işlemini adım adım anlatalım.

Adım 1:

İlk olarak aircrack programını internetten indirelim. Bunun içim ya Ubuntu Software center kullanabiliriz Ya da terminalden "wget" komutunu kullanabiliriz.

sudo wget <program internet adresi>

#sudo apt-get install aircrack-ng 1. 0

Programımız şuan sisteme kuruldu.

Adım 2:

Terminalden aşağıdaki komutu yazarak sistemimizin kablosuz erişim kartının bu program için desteklenip desteklenmediğini test etmeliyiz.

#sudo airmon-ng

#sudo airmon-ng start wlan0

Yukarıdaki komut ile Atheros çipsetli wlan0 arayüzlü kablosuz istemcimizin monitör modunda çalışmasını sağlıyoruz.

#sudo airmon-ng start mon0

Artık monitör modda paketleri dinleyebiliriz. Fakat aircrack programının resmi sitesine girerseniz çipsetinizin desteklendiği görürseniz mon0 yerine wlan0 ile paket dinleyebilirsiniz.

Adım 3:

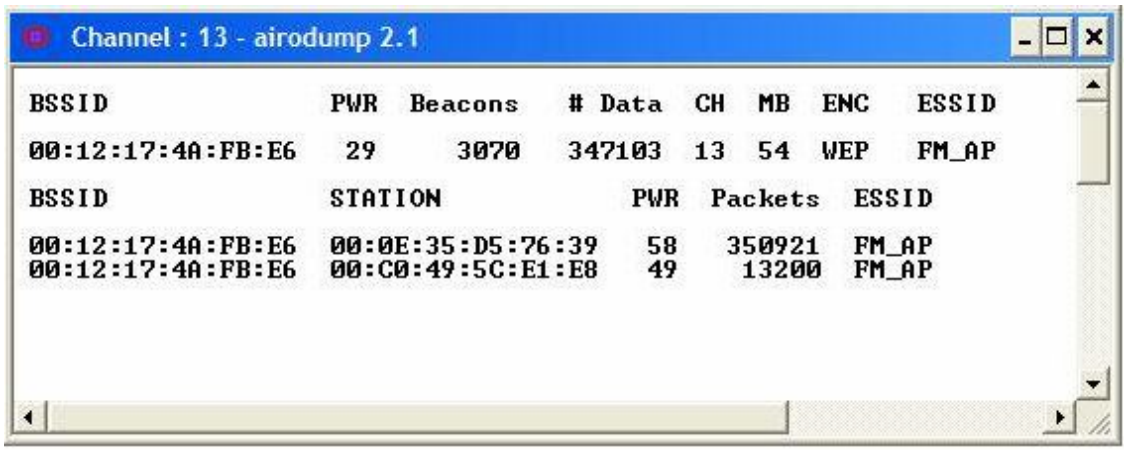
Bu adımda artık dinleyeceğimiz AP'nin Mac adresini ve kanalını bulduk. Artık hedefe giden paketleri dinleyelim.

#sudo airodump-ng –c 11 –b 00:1A:2B:66:D4:B5 –w dmg mon0

-c --> channel

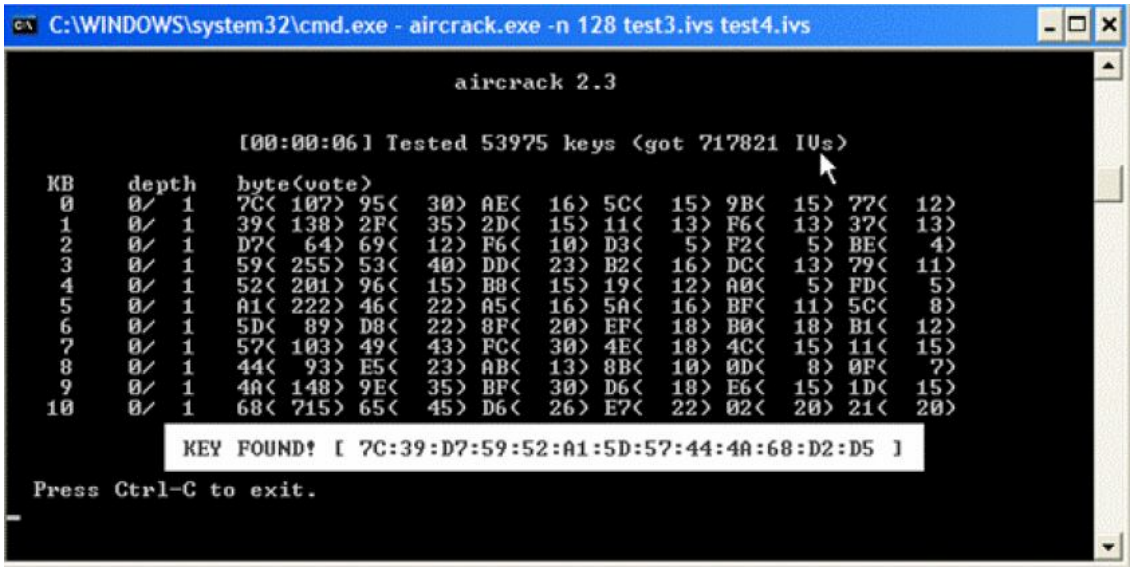
-b --> BSSID

-w write anlamına gelir. Burda "dmg" ise paketlerin (IVS) toplanacağı dosyadır.



Şekil 4. 1. Airodump Programı Paket Toplama Ekranı

sudo aircrack-ng dmg. ivs(cap) , bu komuttan sonra istenilen AP'nin index numarası girilir.



Şekil 4. 2. Aircrack Programı Şifre Bulunma Ekranı

4.2 Wpa-Psk Şifrelemesinin Aircrack Programı İle Kırılması

WPA-PSK şifrelemesi kullanan erişim noktalarına Brute force atak yapılarak, kablosuz ağın şifresi elde edilebilir. Burada önmeli olan 2 nokta vardır. Bunlardan birinci Handshake (tokalaşma) yakalamak ve iyi bir kelime listesine sahip olmaktır. Bu kelime listelerini internetten indirebilir Ya da kendimiz olauşturabiliriz.

Bu uygulamamız için işletim sistemi olarak Linux türevi ve en popüler olan Ubuntu LTS 10.0.3 kullanılmıştır. Şifre kırma programı olarak aircrack-ng 1. 0 programı kullanılmıştır. Şifre kırma işlemini adım adım anlatılmıştır.[Ohigashi T., Morii M.,2009]

Adım 1:

İlk olarak aircrack programını internetten indirelim. Bunun içim ya Ubuntu Software center kullanabiliriz Ya da terminalden “wget” komutunu kullanabiliriz.

sudo wget <program intenrnet adresi>

#sudo apt-get install aircrack-ng 1. 0

Programımız şuan sisteme kuruldu.

Adım 2:

Terminalden aşağıdaki komutu yazarak sistemimizin kablosuz erişim kartının bu program için desteklenip desteklenmediğini test etmeliyiz.

#sudo airmon-ng

#sudo airmon-ng start wlan0

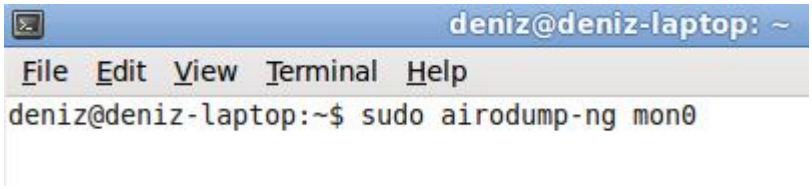
Yukarıdaki komut ile Atheros çipsetli wlan0 arayüzlü kablosuz istemcimizin monitör modunda çalışmasını sağlıyoruz.

#sudo airmon-ng start mon0

Artık monitör modda paketleri dinleyebiliriz. Fakat aircrack programının resmi sitesine girerseniz çipsetinizin desteklendiği görürseniz mon0 yerine wlan0 ile paket dinleyebilirsiniz.

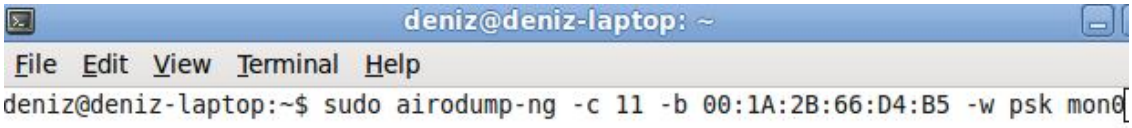
Adım 3:

Bu adımda artık dinleyeceğimiz AP'nin Mac adresini ve kanalını bulmak için aşağıdaki komut çalıştırılır.



Şekil 4. 3. Airodump Monitör modu Çalışma Komutu

Buradan şifresini bulmak istediğimiz AP'nin Mac adresini ve kanalını tespit ettik.

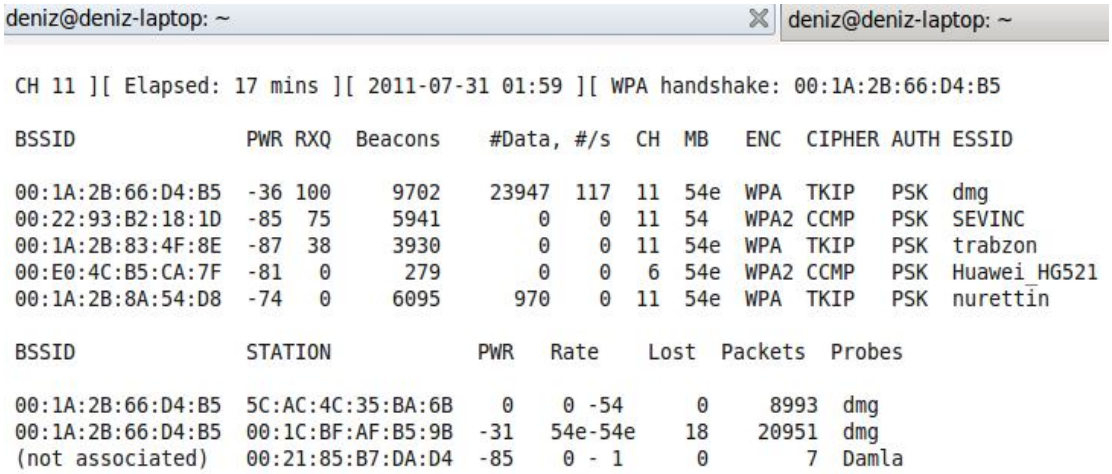


Şekil 4. 4. Airodump Komutu ile Belirlenen AP'den paket toplama

-c --> channel

-b --> BSSID

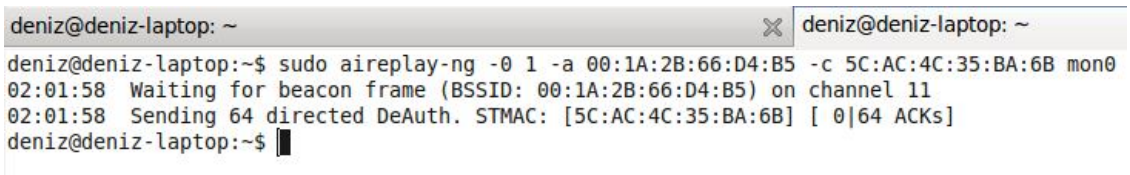
-w write anlamına gelir. Burda psk ise paketlerin toplanacağı dosyadır.



Şekil 4. 5. Paket Toplama Ekranı (AP listesi)

Adım 4:

WPA-psk şifresini bulurken önemli olan handshake yakalamaktır. Bunun içinde aşağıdaki komut ile handshake bulmaya sistemi zorlayabilirsiniz.



Şekil 4. 6. Aireplay Komutu ile Deauth Atak komutu

Bu komut ile istasyona, istemciden Deauth mesajları gönderiyor. Amaç handshake yakalamaktır.

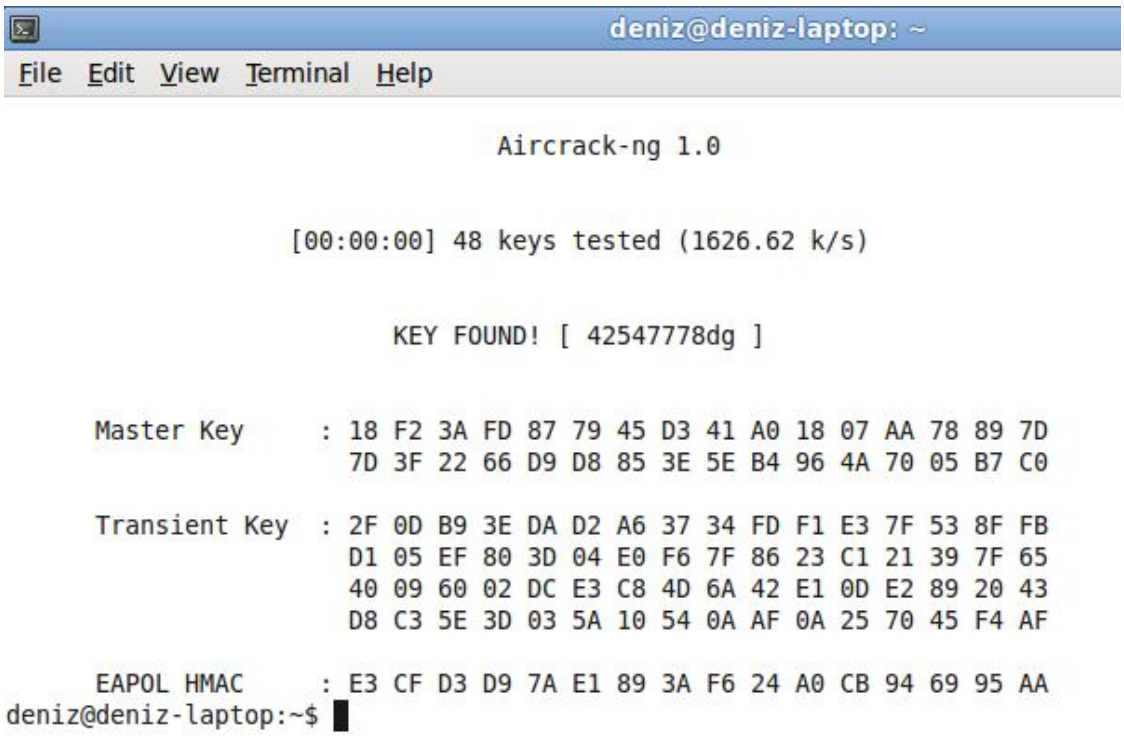
Adım 5:

Paketlerimizi topladıktan sonra ve tokalaşma yakaladıktan sonra bu psk adlı dosyayı aircrack programı ile çalıştırıyoruz.



Şekil 4. 7. Aircrack ile toplanan paketlerden şifre Elde etme

Şansınız varsa ve iyi bir kelime listesinize sahipseniz şifreyi bulabilirsiniz. Bizim uygulamamız da şifremiz elde edilmiştir.

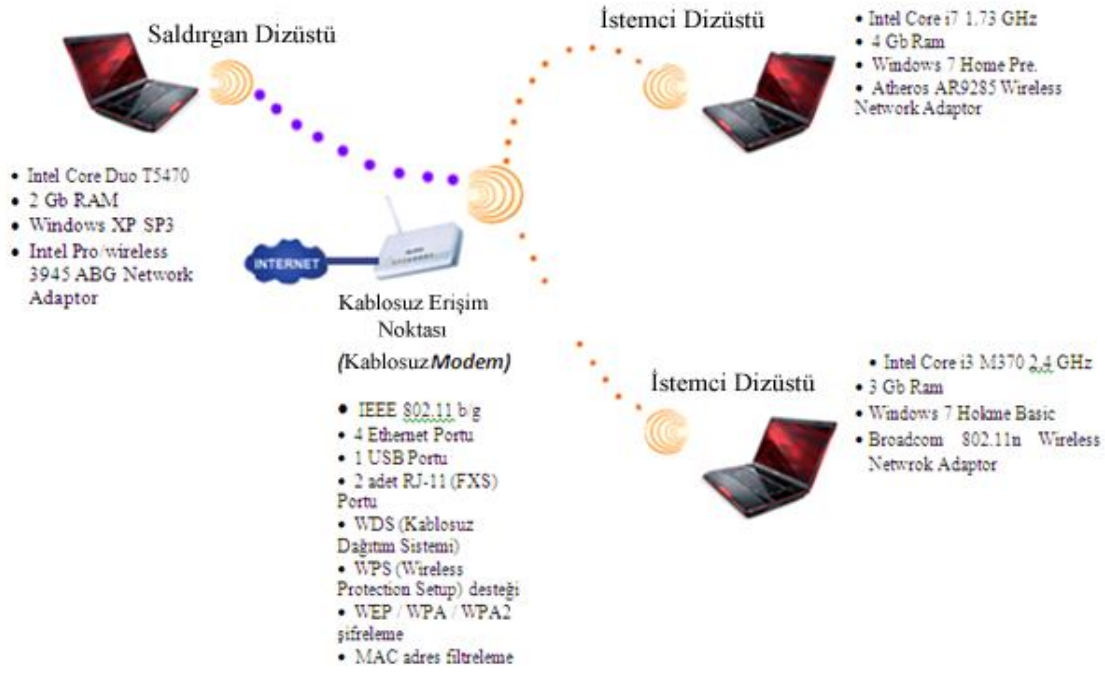


Şekil 4. 8. WPA-PSK Şifresinin Bulunma Ekranı

4.3 Oluşturulan Bir Kablosuz Ağ Ortamı İle Gerçekleştirilen DoS Atak Uygulamaları

4.3.1 Test Ortamı

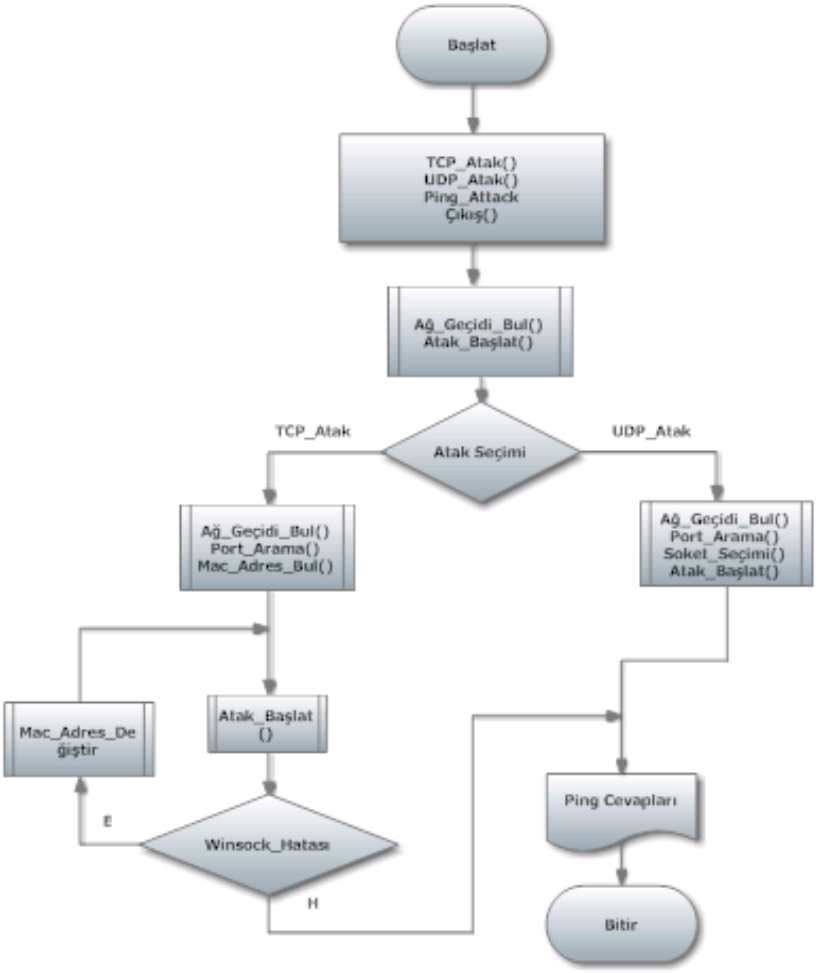
Deneysel çalışmada gerçek bir kablosuz ağ ortamından yararlanılmıştır. Çalışmada bir adet 802.11g (802.11b uyumlu, 2. 4 GHz Aralığında, 54 Mbps'e kadar çıkan hız kapasitesi) içeren erişim noktası ve aynı zamanda kablosuz modem görevi gören bir cihaz kullanılmıştır. Bunun yanında 3 adet taşınabilir bilgisayar, biri saldırgan olarak diğer ikisi yasal kullanıcı olarak bu kablosuz erişim noktasından internete girebilmektedir. Deneysel çalışma için kullanılan bir kablosuz modem(erişim noktası) ve 3 taşınabilir bilgisayarın özellikleri aşağıda Şekil 4. 9.'da gösterilmiştir.



Şekil 4. 9. Test Ortamı

4.3.2 Kullanılan Saldırı Teknikleri

Programda bölüm 3'de açıklanan saldırı türlerinden TCP Data Replay Flood ile Ping Flood saldırı teknikleri kullanılmıştır. TCP Data Replay Flood ile AP'yi TCP paketlerine boğarken, aynı anda aynı AP'ye büyük ping paketleri göndererek AP'nin diğer kullanıcılara artık servis verememesi ya da internet erişimimin zayıflaması amaçlanmıştır. Teknikler kullanırken TCP ve ping gibi protokol ve komutların açıkları kullanılmıştır. Programın Windows ortamında arka planda gizli çalışması sağlanılmıştır. Program modüler yapıdadır. AP'ye bağlantı için Winsock. dll dosyası kullanılmıştır.



Şekil 4. 10. Programın Akış Diyagramı

4.3.2.1 Tcp Veri Tekrarı Taşması Saldırısı (Tcp Data Replay Flood Attack)

Başlangıçta TCP Flood saldırısı denenildi. Saldırı için öncelikle Gateway'in (Access Point) adını, Ip adresini ve Mac adresini windows ortamında bulunan ipconfig komutuyla bulundu (Gateway_Find() fonksiyonu). Bulunan gateway'in portları port_search() fonksiyonu ile taranarak açık olanları tespit edilmeye çalışıldı. Genellikle AP'de ya da kablosuz modemlerde bu saldırıları önlemek amacıyla başlangıçta portlar kapalı olarak satın alınır. Ancak bazı temel uygulamalar bazı portları (örnek: 21, 23, 80 gibi) kullandığından bu portlar açık gelmektedir. [Port Numaraları,2002]. Daha sonra attack_start() fonksiyonu ile saldırı yapılmıştır. Saldırı karşı makine tarafından anlaşıldığında Mac_adres_change() [Macshift,2004] fonksiyonu ile mac adresi değiştirilip saldırı hizmet durana kadar tekrarlanmıştır. Tek başına bu saldırı etkisiz kalmaması için ping Flood Attack ile aynı zamanda çalıştırılmıştır.

```
Winsock nesnesini açıksa kapat ve Aç.
…
lblportsayac. Caption = Int(lblportsayac. Caption) + 1
Sayacı devamlı arttır ve AP'ye bağlanmaya çalış
Winsock2.RemoteHost = txtHost. Text
Winsock2.RemotePort = lblportsayac. Caption
Winsock2.Connect
…
Bağlandığında o port açıktır. Bunu listele.
```

Şekil 4. 11. AP bulma ve Açık port Arama Pseudo Kodları

Servis Adı	Port Numarası/Protokol	Servis İsmi Açıklaması
ftp	21/tcp	File Transfer [Control]
ftp	21/udp	File Transfer [Control]
Telnet	23/tcp	Telnet
Telnet	23/udp	Telnet
http	80/tcp	World Wide Web HTTP
http	80/udp	World Wide Web HTTP
www	80/tcp	World Wide Web HTTP
www	80/udp	World Wide Web HTTP
www-http	80/tcp	World Wide Web HTTP
www-http	80/udp	World Wide Web HTTP

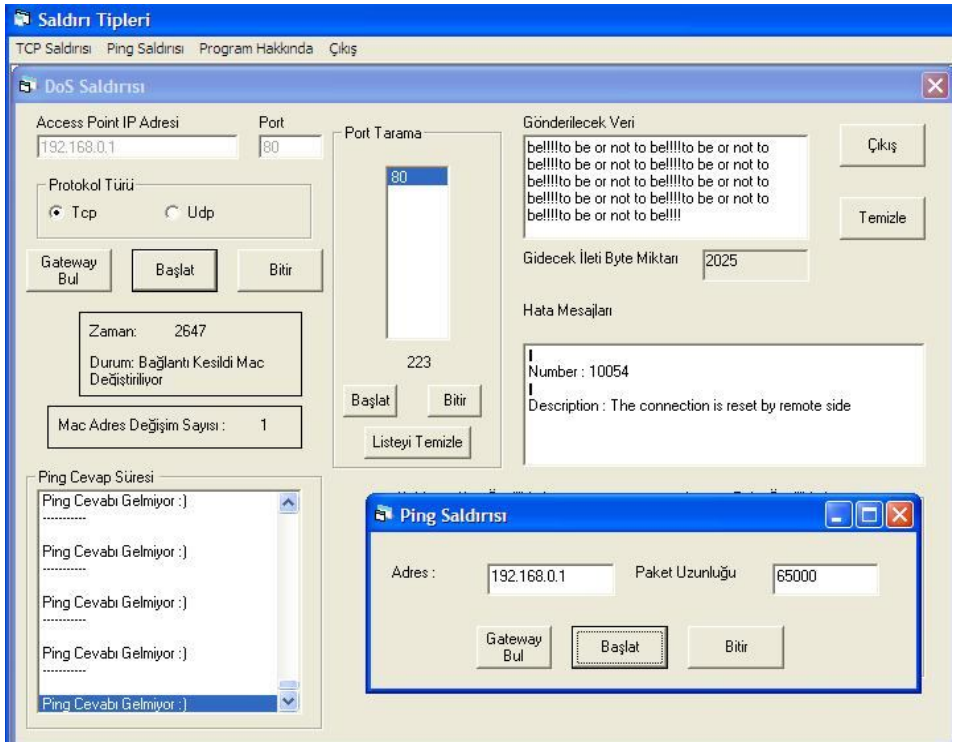
Tablo 4. 1. Saldırı için Açık olan bazı portlar

```
Gateway adresi Mac Bulma fonksiyonuna girdi oluyor.
…
If SendARP(dwRemoteIP, 0&, pMacAddr, PhyAddrLen) = NO_ERROR Then
        If pMacAddr <> 0 And PhyAddrLen <> 0 Then
           ReDim bpMacAddr(0 To PhyAddrLen - 1)
           CopyMemory bpMacAddr(0), pMacAddr, ByVal PhyAddrLen
           For cnt = 0 To PhyAddrLen - 1
              If bpMacAddr(cnt) = 0 Then
                 tmp = tmp & "00-"
              Else
                 tmp = tmp & Hex$(bpMacAddr(cnt)) & "-"
              End If
           Next
            If Len(tmp) > 0 Then
              sRemoteMacAddress = Left$(tmp, Len(tmp) - 1)
              Mac_Adress_Find = True
           End If
            Exit Function
        Else
           Mac_Adress_Find= False
        End If
     Else
        Mac_Adress_Find = False
     End If
…
…
```

Şekil 4. 12. Mac Adresi Bulma Fonksiyonun Pseudo Kodları

```
Winsock state değerimiz 0 olmadığı sürece saldırı yap.
…
If Winsock1.State <> 0 Then
     Winsock nesnesi ile veri gönder.
            Winsock1.SendData txtData. Text
Sayacı arttır.
            lblSent. Caption = lblSent. Caption + 1
…
Bağlantı koparsa ya da AP bizi atarsa Mac adres değiştir tekrar bağlan.
Saldırı ya devam et.
…
   lblStatus. Caption = "Durum: Bağlantı Kesildi Mac Değiştiriliyor"
…
Mac Değiştir Fonksiyonunu çalıştır.
…
Macdegistir()
```

Şekil 4. 13. Atağı Başlatma Pseudo Kodu



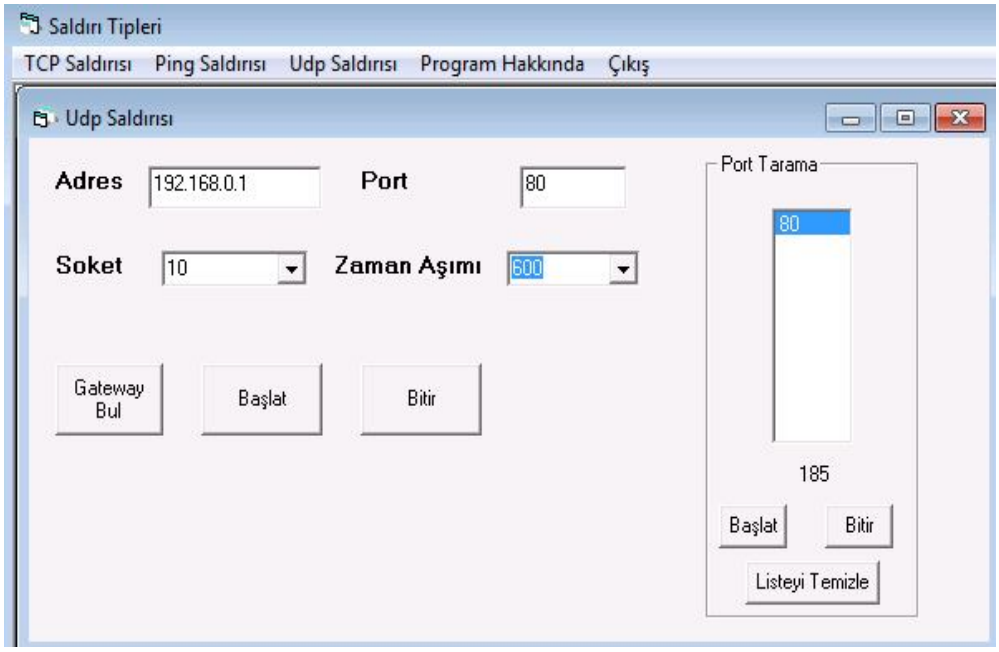
Şekil 4. 14. Saldırı sonuç örneği ekranı

4.3.2.2 Ping Taşması Saldırısı (Ping Flood Attack)

Ping Flood saldırısı yapmak için tekrar gateway_find() fonksiyonu çağrılmıştır. Gateway adresi bulunduktan sonra istediğimiz değer kadar veri paketleri AP'ye gönderilmiştir. Bu çalışmada bu başlangıç değeri 65000 olarak belirlenmiştir. Bu adımdan sonra atak başlatılmıştır.

```
Gateway bul.
…
Bu AP'ye 65000 boyuntunda ping paketleri yolla.
…
Shell "ping " + (Text1.Text) + " -n1 -l " + (Text2.Text) + " & exit", vbHide
…
Devamlı Tekrarla.
```

Şekil 4.15. Programın Access Point'te ping saldırısını başlatması için gerekli kod



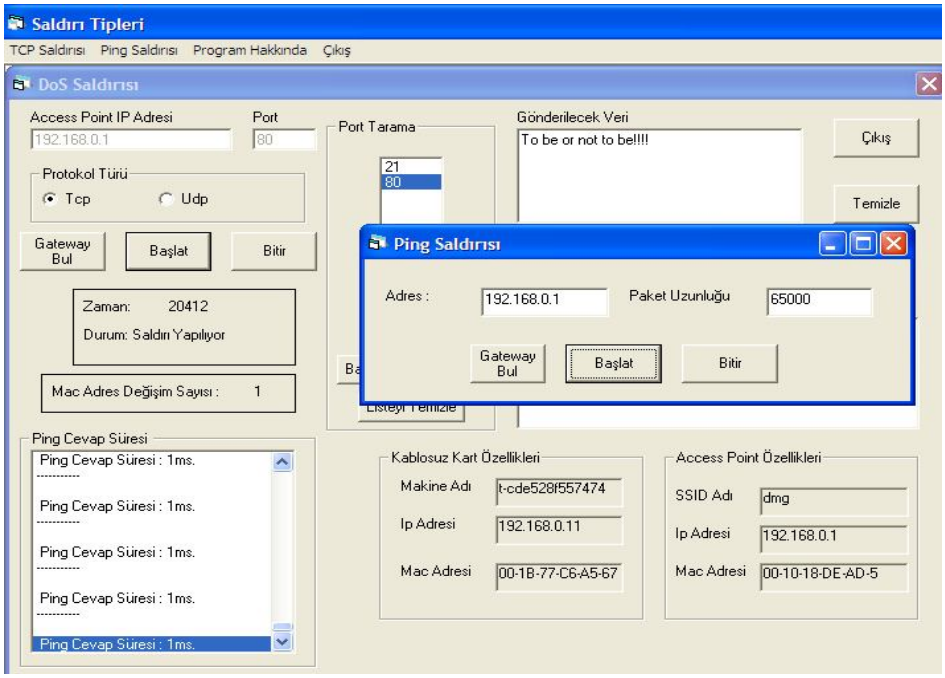
Şekil 4.16. Udp Taşma Saldırı Ekranı

```
1'den istenilen soket kadar döngü kur.
…
        Load Winsock1(i)
        Next i
 …
Bu soketleri yükle.
…
        Timer1.Interval = CInt(Combo2.Text)
        Timer1.Enabled = True
…
İstenilen veriyi port üzerinden gönder.
…
   With Winsock1(i)
     .Close
     .Connect txtAdres. Text, CInt(txtPort. Text)
     .SendData dmg
   End With
```

Şekil 4.17. Udp Flood saldırısını başlatmak için gerekli kod

4.3.2.3 Udp Taşması Saldırısı (Udp Flood Attack)

Udp flood saldırısı yapmak için tekrar gateway_find fonksionu çağrılmıştır. Daha sonra, açık olan portları bulmak için port_search fonksiyonu çağrılmıştır. Bu işlemlerden sonra istediğimiz soket ve zaman aşımı seçenekleri seçilmiştir. Bu adımdan sonra atak başlatılmıştır.

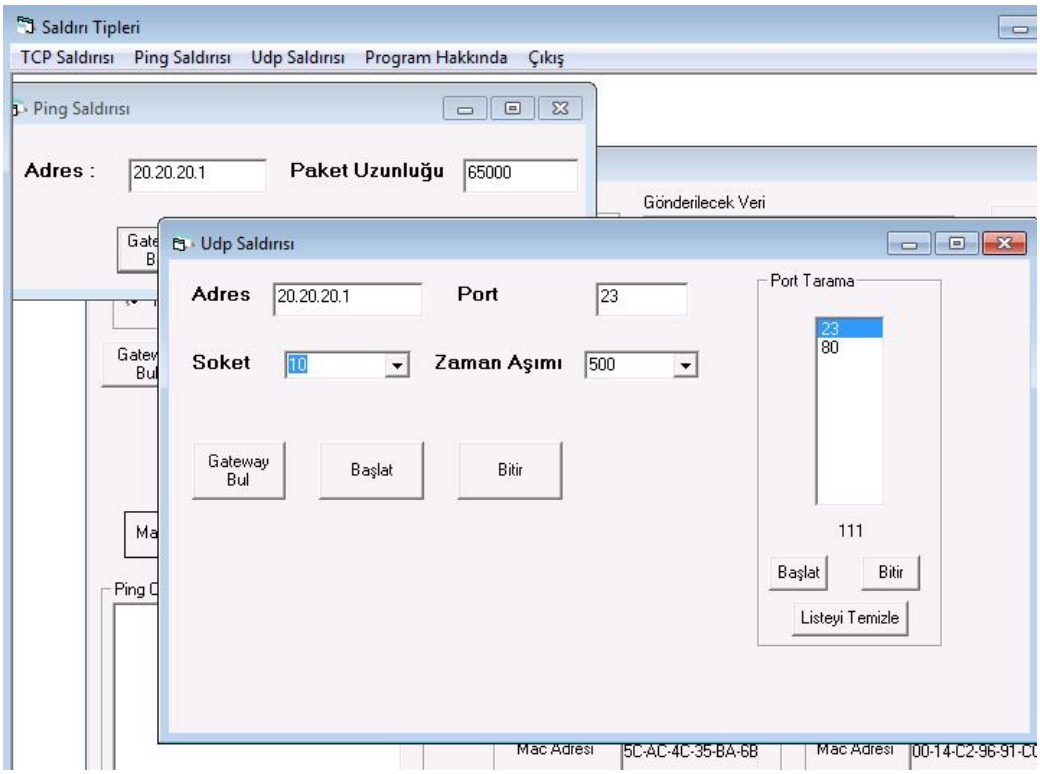


Şekil 4.18. TCP ve Ping Taşması Saldırısı Program Ekranı

Programda TCP protololü üzerinden 512 byte, 1024 byte veri gönderilirken aynı zamanda ping saldırısı ile aynı gateway adresine 65000 bit uzunluğunda ping paketleri gönderildi. Gönderilen veri büyüklüğü arttırılıp birden çok makine üzerinden gönderildiğinde (zombie bulduğumuzda) programın etkinliği artığı ve bir süre sonra cihazın devre dışı kaldığı gözlenildi.

4.3.3 Dwl–2100 AP Cihazına Yapılan Saldırı Örneği

Dwl–2100 AP cihazına saldırılmıştır. Program çalıştırıldığında kablosuz cihazın IP adresinin 20.20.20.1 olduğu ve açık portlarının 23 ve 80 olduğu tespit edilmiştir.

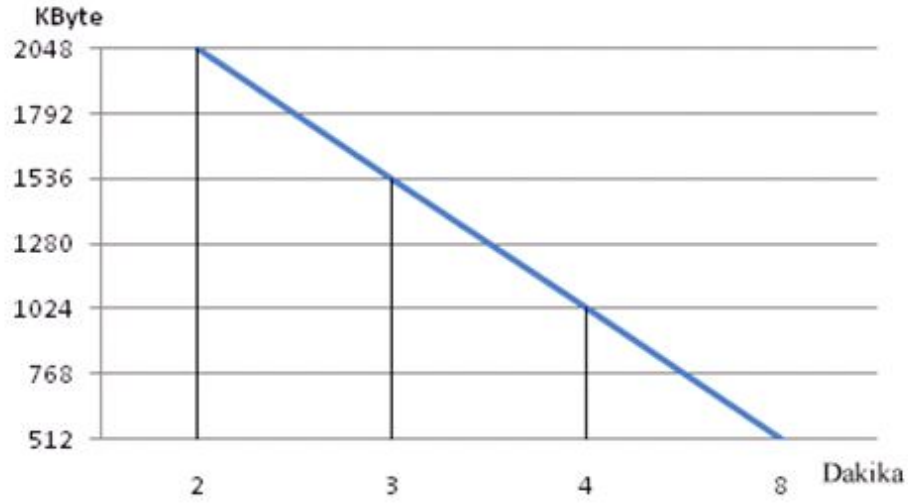


Şekil 4.19. Ping ve Udp Taşması Saldırısı Program Ekranı

Programda gateway adresine 65000 bit uzunluğunda ping paketleri gönderilmiştir. Aynı zamanda istenilen soket sayısı kadar açık olan portlardan belirli aralıklarda UDP paketleri gönderilmiştir. Gönderilen veri büyüklüğü arttırılıp birden çok makine üzerinden gönderildiğinde (zombie bulduğumuzda) programın etkinliği artığı gözlenilmiştir. Bir süre sonra cihazın sağladığı internetin yavaşladığı ve ping cevaplarının gelmediği izlenilmiştir.

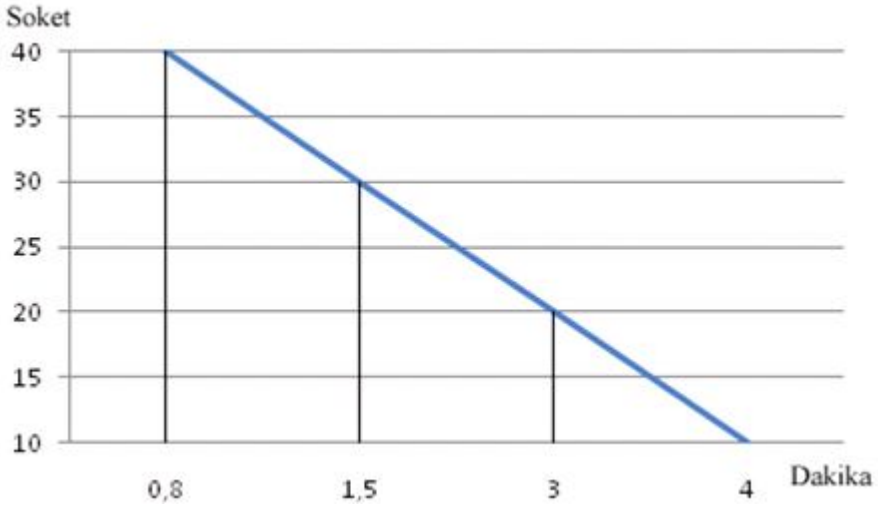
4.3.4 DoS Saldırısı Deney Sonuçları

Yapılan saldırılar sonucunda elde edilen deney sonuçları Şekil 4.20. ve 4.21. de verilmiştir. İlk saldırımız Netmaster Kablosuz modem ve AP'ye yapılmıştır. Bu ataklarda Zombie kullanılmamıştır. Bu cihaza uygulanan ataklar TCP Data Replay ve Ping saldırısıdır.



Şekil 4.20. Netmaster Kablosuz Modem Cihazına Yapılan Saldırı Sonuçları

İkinci saldırımız Dlink AP'ye yapılmıştır. Bu cihaza uygulanan atak UDP Flood ve Ping saldırısıdır.



Şekil 4.21. Dwl–2100 AP Cihazına yapılan Saldırı Sonuçları

Şekil 4.20 ve Şekil 4.21'de ki grafiklerden açıkça görüleceği gibi her iki saldırıda da gönderilen veri miktarı arttığında cihazların devre dışı kalma süreleri azalmaktadır. Saldırının kısa sürede amacına ulaşabilmesi için gönderilen veri miktarı mümkünm olduğu kadar yüksek seçilmesi gerekmektedir. Ayrıca birden fazla bilgisayardan aynı saldırı gerçekleşirse cihazların devre dışı kalma süresi daha da azalacaktır.

5.SONUÇLAR

Sonuç olarak tezimize başladığımız 2007 yılından bu yana kablosuz ortamlardaki gelişmeler doğrultusunda kablosuz ağ yelpazesi genişlemiştir. Kablosuz yerel ağlarda 802.11g cihazların hâkimiyeti yavaş yavaş sona erip 802.11n cihazları piyasaya yayılmaktadır. 802.11n standardının desteklediği kablosuz ağ cihazlarında yeni geliştirilen MIMO teknolojisini kullanılmaktadır. Bu da yüksek hız (300 Mbp/s) ve daha geniş kapsama alanı anlamına gelmektedir. Kablosuz ağların güvenliği açısından da gelişmeler kaydedildi. Erişim Noktalarında WEP şifrelemesi olmasına rağmen kullanımından hemen hemen vazgeçilmiştir. Bunu yerini TKIP destekli WPA, AES destekli WPA2 ve 802.1X asıllama sunucuları kullanılması ön plana çıkmıştır. Eskiye dönük Erişim Noktalarında da içinde bulunan yazılımlar(firmware) güncellenmiştir. Kablolu ağların başını fazlaca derde sokan, çoğu web sitesinin çalışmasını engelleyen aksatan DoS ataklar, Kablosuz Ağlar için de sorunlar teşkil etmektedir. DoS ataklar tam anlamıyla önlenemese bile bu ataklara karşı Erişim noktaları yazılımları geliştirilmiş ve Saldırı Tespit Sistemleri piyasaya çıkmıştır. Böylece kablosuz iletişimin ilk yıllarına göre güvenlik ve erişim standarları gelişme göstermiştir.

Bu tezde de 802.11n standardı ile gelen yapısal değişikler incelenmiştir. Diğer eskiye dönük standartlarla karşılaştırılarak sonuçlar çıkarılmıştır. Bu sonuçlara göre Kablosuz yerel alan ağlarının artık 802.11n standardına göre planlanmasının gerektiği anlaşılmıştır. Güvenlik açısından tüm güvenlik politikaları incelenmiş WEP ve WPA-PSK şifreleme yapısının nasıl kırıldığı gösterilmiştir. Bu sonuçlara göre Erişim noktalarında AES tabanlı WPA2 kullanılması gerektiği anlaşılmıştır. Son olarak tezde DoS atak programı yapıldı ve bir kablosuz modem ve erişim noktası üzerinde etkisi

denendi. Sonuç olarak Erişim noktlarının kablosuz modemelere göre daha güvenliş olduğu ve daha çok güvenlik politikası içerdiği anlaşıldı. Güvenliğin çok gerektiği ortamlarda DoS ataklarına karşı gömülü firewall yazılımı olan cihazlar alınmasının şart olduğu ve eskiye dönük erişim noktalarının güncellenmesi gerektiği anlaşılmıştır.

KAYNAKLAR

Aircrack, 2009, http://www.aircrack-ng.org/

Aravamudhan L., 2003 , "Getting to Know Wireless Networks and Technology"

ARRLWeb: " Part 97 - Amateur Radio Service. American Radio Relay League", 2001, www.arrlg.org

Bahai, A. R. S., Saltzberg, B. R., Ergen, M.,, 2004, " Multi Carrier Digital Communications: Theory and Applications of OFDM", Springer.

Barnes, C., Bautts T., Lloyd D., Ouellet E., Posluns, J., Zendzian, D.M., O'Farrel, N., 2002, "Hack Proofing Your Wireless Network. Syngress Publishing Inc"

Borsc M., Shinde H., 2005 ,"Personal Wireless Communications, 2005. ICPWC 2005. 2005 IEEE International Conference on", 0-7803-8964-6, 23-25

Bluetooth Haberleri, 2008, http://www.bluetooth.com/Pages/Bluetooth-Home.aspx

Bluetooth 3.0 – 4.0 Yapısı , 2010, http://www.agciyiz.net/index.php/kablosuz-aglar/bluetooth–3-0-bluetooth-4-0/

Chang, R. W., 1996, "Synthesis of band limited orthogonal signals for multi channel data transmission", Bell System Technical Journal 46, pp.1775-1796

CISN (Computing & Information Services Newsletter), 2002, http://cisn.odtu.edu.tr/2002-6/ieee.php

Computer Security, 2001, Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899–8930

Daemen J., Rijmen V., 1998, "AES Proposal: Rijndael, First Advanced EncryptionConference", California

Dos Saldırıları, 2009, http://www.us-cert.gov/cas/tips/ST04-015.html

Dubendorf V.A. , 2003 ,"Wireless Data Technologies", Jhon Wiley & Sons, Ltd ISBN: 0-470-84949-5

Dubuc C., Starks D., Creasy T., Hou Y., ,2004 , "A MIMO-OFDM prototaype for next-generations wireless WANs", IEEE Communications Magazine, vol.42, pp.82-87

Eklund C., Roger B. M., Kenneth L. ,Wang S.S., 2002, IEEE Standard 802. 16: "A Technical Overview of the WirelessMAN™ Air Interface for Broadband Wireless Access", 0163-6804/02/$17.00 © 2002 IEEE, IEEE Communications Magazine

ETSI, ETSI HIPERLAN/1 Standart, Future Devolopmans
http://portal.etsi.org/bran/kta/Hiperlan/hiperlan1.asp,28.02.2004

ETSI, ETSI portal, BRAN, ETSI HIPERLAN/2 Standard, Overview
http://portal.etsi.org/bran/kta/Hiperlan/hiperlan2.asp,28.07.2004

ETSI, ETSI portal, BRAN, Hiperlan2, hiperaccess,
http://portal.etsi.org/bran/Summary.asp, 28.07.2004

Eusso Quality Network, http://www.eusso.com/Models/Wireless/UGL2454-VPA/UGL2454-VPA.htm

FIPS 197, 2001, Advanced Encryption Standard, Federal Information Processing Standard(FIPS), Publication 197, National Bureau of Standards, U.S. Department of Commerce, Washington D.C.

Fluhrer S., Mantin I. and Shamir A., 2001, “Weaknesses in the Key Scheduling Algorithm of RC4” , Lecture Notes in Computer Science, Volume 2259/2001, 1-24, DOI: 10.1007/3-540-45537-X_1

Geier J. ,2006, “Overview of the 802. 11 Standard”, http://www.wireless-nets.com

Geier, J., 2002, “Wireless LANs, Wireless System Entegration”, Second edition, Chapter 6, İndiana, ABD, s.1, 5, 7-10, 13,

Gezgin D.M., Buluş E., Buluş H. N. “The security suggestıons for wireless access points”,Yambol,2009

Gezgin D.M., Buluş E., Buluş H.N., 2008 ,“The Technical Analysis of the Comparison of 802.11n Wireless Network Standard”, International Scientific Conference, Gabrovo

Gezgin D.M., Buluş E., 2009, "RC4 tabanlı WPA(wi-fi protected Access)'da kullanılan TKIP (Temporal Key Integrity Protocol) şifrelemesinin incelenmesi", itusem 2009, 107-112 pp., Adana, Türkiye

Gezgin D.M., Buluş E., 2008,“Kablosuz Erişim Noktalarına Yapılan DOS Saldırıları”, Akademik Bilişim 2008, Çanakkale

Goldsmith A.. 2006, “Overview of Wireless Communications ”, Wireless Communications,http://www.cambridge.org/us/catalogue/catalogue.asp

GPRS,2011,http://www.teknovadi.com/cep-telefonu-rehberi/gprs-nedir-ve-nasil-calisir-gprs-network-ve-yapisi

GSM World, 2011,http://www.gsm.org/

Holma H.,Toskala A., 2000, “WCDMA for UMTS Radio Access For Third Generation Mobile Communications”

HomeRF Working Group, http://www.palowireless.com/homerf/homerf1.asp

IEEE 802. 11: Wireless Local Area Networks, 2011, http://standards.ieee.org/about/get/802/802.11.html

IEEE,2003,http://standards.ieee.org/getieee802/download/802.11F–2003.pdf

IEEE 802.11n Standardı,2011, http://www.cisco.com/en/US/netsol/ns767/index.html

IEEE 802. 20 MBWA,2005,http://www.ieee802.org/20/

HomeRf,2002,http://www.palowireless.com/homerf/homerf1.asp

IEEE,2008,“WirelessStandartsZone”,http://standards.ieee.org/wireless/overview.html

IEEE,802.11a-1999 High-speed Physical Layer in the 5 GHz band (1999-02-11). Retrieved on 2007-09-24.

IEEE, 802. 11b-1999 Hiher Speed Physical Layer Extension in the 2.4 GHz band 2007-09 -24

IEEE 802.11g-2003: Further Higher Data Rate Extension in the 2.4 GHz Band . IEEE (2003-10-20).

IEEE 802.11i-2004: Amendment 6: Medium Access Control (MAC) Security Enhancements" (pdf). IEEE Standards. 2004-07-23

IEEE Standard Association, http://standards.ieee.org/about/get/802/802.11.html

IEEE 802. 11 Working Group IEEE 802. 11-2007: Wireless LAN Medium Access Control (MAC) and Physical Layer Specifications. ISBN 0-7381-5656-9.

IEEE 802 Working Group & Executive Committee Study Group Home Pages,2011, www.ieee802.org/dots.shtml

Infrared,2011,Infrared Data Association Home Page, www.irda.org

Johnsson, M., 1999, HiperLAN/2 Global Forum, HiperLAN2 – The Broadband Radio Transmission Technol,200ogy Operating in the 5 GHz Frequency Band

Kablosuz Ağ Standardları, 2003, http://www.bidb.itu.edu.tr/?d=954

Kablosuz Anten Çeşitleri, 2002,
http://idari.isikun.edu.tr/bim/en/bilgiarsivi/arsiv/wireless.php

Kablosuz Teknoloji, 2005, http://www.netsis.com.tr/goksel/Wireless/Wt.HTM

Kaminski C. Technology overview of HomeRF 2. 0, , 15-May–2001,
http://www.homenethelp.com/web/explain/about-homerf-2b.asp

Kaplan Y, 2002, "Kablosuz LAN teknolojileri"

Kavas A., ,2006 ,"Geniş Bantta Telsiz Erişim: WiMAX", Yıldız Teknik Üniversitesi Elektrik-Elektronik Fakültesi

Kim Y.M., 2003, "Ultra Wide Band (UWB) Technology and Applications', The Ohio State University

Lisa P., 2009,"A list of wirelises network attacks", SearchSecurity.com

Macshift: , 2004, Change your MAC address, http://devices.natetrue.com/macshift/

Matsui M., 1994.,"Linear Cryptanalysis Method for DES Cipher, Advances in Cryptology-EUROCRYPT' 93", pp. 386-397, Springer-Verlag

Matthew S.G, 2005, “ 802. 11 Wireless Networks: The Definitive Guide”, Second Edition

Molisch F., Foerster J.R., Pendergrass M., 2003, “Channel Models for Ultrawideband Personal Area Networks”, vol. 10, pp.14-21. , IEEE Wireless Com

Ohigashi T.,Morii M. ,2009, “A Practical Message Falsi_cation Attack on WPA”, http://jwis2009.nsysu.edu.tw/location/paper/A Practical Message Falsification Attack on WPA.pdf

Öztürk E., 2004, “Wlan Kablosuz Yerel Alan Ağları (Wıreless Local Area Networks) Teknolojisinin İncelenmesi, Mevcut Düzenlemelerin Değerlendirilmesi Ve Ülkemize Yönelik Düzenleme Önerisi”.Telekomünikasyon Kurumu

Patil B., 2003, IP in Wireless Networks, Chapter Eleven, IP in 802.11 Networks, Pearson Education Ltd., London

PortNumaraları, 2002, http://www.iana.org/assignments/port-numbers, last updated 2011-04-29

Rahman L.F., Zhou R., “ Ip Address Spoofing” , Albert-Ludwigs-Universität Freiburg, Institute for Computer Science,2003

Ritz J.A., 2003, Introduction to the 802.11 Wireless Network Standard.CyberScience Laboratory, Rome

Safaric, S. Malaric, K., 2006,"ZigBee wireless standard", 48th International Symposium ELMAR-2006, pp.259-262, Zadar, Croatia

Scarfone K., Dicoi D.,Sexton M., Tibbs C., “Guide to Securing Legacy IEEE 802. 11 Wireless Networks”,

SearchNetworking com, Definitions, HomeRF, http://searchnetworking.techtarget.com/sDefinition/0sid7_gci53509200.html

Tanenbaum A., Computer Networks, 4. sürüm, 2003

TCP And UDP, 2001, By Steve Steinke, Network Magazine http://www.networkmagazine.com/article/NMG20010126S0005

TCP Tokalaşması, 2002, http://www.texascollaborative.org/SmithModule01/sec1_con.php

Tews E.,Weinmann R., Pyshkin A., 2007 ,"Breaking 104 bit WEP in less than 60seconds", Cryptology ePrint, available at http://eprint.iacr.org/2007/120.pdf

The sensible guide to 802.11y, 2008,http://www.sensibleradio.com/11y.pdf

Tjensvold J. M., 2007 ," Comparison of the IEEE 802. 11, 802.15.1, 802.15.4 and 802.15.6 wireless standards"

UGL2454-VPA,2005, http://www.eusso.com/Models/Wireless/UGL2454-VPA/UGL2454-VPA.htm

Ultra Wide Band Wireless Data Transfer Technology,2007, Ixbt Labs, http://ixbtlabs.com/articles2/uwb/

Yang F.,Zhou F.,Zhang L.Feng J., 2005, "An improved security scheme in WMAN based on IEEE standard 802. 16",pp. 23-26, IEEExplore

Yoshio K., Tetsuki T., 2002, "On Multiple-Input-Multiple-Output (MIMO) Maximal Ratio Combining (MRC) and Optimal Data Transmission for OFDM", pp. 45-52

ZigBee Birlikteliği (ZigBee Alliance) websitesi,2006, http://www.zigbee.org

WPA and WPA2 Implementation White Paper, 2005,“ Deploying Wi-Fi Protected Access (WPA™) and WPA2™ in the Enterprise”
WPA 802.1X Port Tabanlı Kimlik Kanıtlama, 2006,
http://www.belgeler.org/howto/p8021x-howto-intro.html

Wright J., ,2003,GCIH, CCNA, “Detecting Wireless LAN MAC Address Spoofing”
802.11 y Standardı,2008, http://www.sensibleradio.com/11y.pdf

Wireless Communication,1995,
http://www.wireless.per.nl/reference/chaptr05/ofdm/ofdm.htm.

Wireless Networks,2008, http://en.kioskea.net/contents/wireless/wlintro.php3

TEZ SIRASINDA YAPILAN ÇALIŞMALAR

ULUSLARARASI KONGRE VE SEMPOZYUM BİLDİRİLERİ

1. D.M.Gezgin, E.Buluş, H.N.Buluş, "The Technical analysis for 802.11x network standards",Unitech'08 , I-287 - I-291 pp., Gabrovo, Bulgaristan, Kasım 2008

2. D.M.Gezgin, E.Buluş, H.N.Buluş, "The Security Suggestions for Wireless Access Points", Pages 133–136, European Dimensions of The Education and Science, Yambol, Bulgaristan, Mayıs 2009

ULUSAL KONGRE VE SEMPOZYUM BİLDİRİLERİ

1.D.M.Gezgin, E.Buluş, "Kablosuz erişim ağlarına yapılan DoS saldırıları", Akademik Bilişim'08, Çanakkale, Türkiye, Şubat 2008

2.D.M.Gezgin, E.Buluş, "Kablosuz Erişim Noktalarında Kullanılan Güvenlik Standartları",UMYOS 2009,Konya, Türkiye, Mayıs 2009

3. D.M.Gezgin, E.Buluş, "RC4 tabanlı WPA(wi-fi protected Access)'da kullanılan TKIP (Temporal Key Integrity Protocol) şifrelemesinin incelenmesi", İTUSEM 2009, 107-112 pp., Adana, Türkiye, Ekim 2009

4.D.M.Gezgin, E.Buluş, "Kablosuz Ağlara Yapılan Saldırılar Ve Türleri: Bir inceleme", Akademik Bilişim'10, Muğla, Türkiye, Şubat 2010

ÖZGEÇMİŞ

Deniz Mertkan GEZGİN, 3 Ekim 1978 yılında Kütahya'da doğdu. İlk, Orta ve Lise öğrenimini Selçuk/İzmir'de tamamladıktan sonra 1995 yılında Çanakkale 18 Mart Üniversitesi Mühendislik Mimarlık Fakültesi Bilgisayar Mühendisliği bölümünü kazandı ve bu bölümden 1999 yılında mezun oldu. 2001 yılı Eylül ayında Trakya Üniversitesi Teknik Bilimler Meslek Yüksek okulunda Öğretim görevlisi olarak çalışmaya başlayan Deniz Mertkan GEZGİN, 2002 senesinde Trakya Üniversitesi Mühendislik Mimarlık Fakültesi Bilgisayar Mühendisliği Bölümünde Yüksek Lisans çalışmalarına başladı ve yüksek lisansını 2006 yılında tamamladı. 2007 yılında Trakya Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Ana Bilim Dalı'nda doktora çalışmalarına başladı. Deniz Mertkan GEZGİN halen Trakya Üniversitesi Eğitim Fakültesi Bilgisayar ve Öğretim Teknolojileri Öğretmenliği Bölümü'nde Öğretim Görevlisi olarak görev yapmaktadır.