T.C.
MALTEPE ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

TEZ ADI

Kablosuz Yerel Alan Ağlarında Güvenliğin İncelenmesi ve Daha Güvenli Hale Getirebilmek İçin Alınacak Önlemler

Öğrenci Adı Soyadı
Fatma ULUCAN

Tez Danışmanı
Prof. Dr. İlhami YAVUZ

İSTANBUL – 2007

T.C.
MALTEPE ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

TEZ ADI

Kablosuz Yerel Alan Ağlarında Güvenliğin İncelenmesi ve Daha Güvenli Hale Getirebilmek İçin Alınacak Önlemler

YÜKSEK LİSANS TEZİ

Öğrenci Adı

Fatma ULUCAN

Tez Danışmanı
Prof. Dr. İlhami YAVUZ

İSTANBUL – 2007

Bu tez çalışması, Maltepe Üniversitesi Fen Bilimleri Enstitüsü Yönetim Kurulu'nun ..... / ..... / ..... tarih ve ..... / ..... sayılı kararıyla oluşturulan jüri tarafından ***Bilgisayar Mühendisliği Yüksek Lisansı Tezi*** olarak kabul edilmiştir.

JÜRİ

Prof. Dr. İlhami YAVUZ
Danışman

Prof. Dr.
Üye

Prof. Dr.
Üye

ÖZET

Bu tezde, kablosuz ağların kapsama alanlarına göre sınıflandırılması yapılmıştır. Kablosuz yerel alan ağları ile ilgili standartları belirleyen 802.11 standardı incelenmiştir. Kablosuz yerel alan ağları için güvenlik ile ilgili olarak tanımlanmış servisler ve protokollerinin özellikleri belirtilmiştir. Bu protokollerin güvenlik açıklarına değinilmiştir ve kablosuz yerel alan ağlarını daha güvenli hale getirecek önlemler incelenmiştir.

Bu tez 2007 yılında yapılmıştır ve 99 sayfadan oluşmaktadır.

Anahtar Kelimeler :WEP, WAP, WAP2, IEEE 802.11, IEEE 802.1X, TKIP, anahtar yönetimi, doğrulama, gizlilik, bütünlük

ABSTRACT

In this thesis, wireless networks according to coverage areas have been classified. Wireless local area network related to standard number 802.11 have been analyzed. Services and protocols related to wireless networks for security purposes have been identified. The security vulnerabilities have been researched and sources to make these wireless networks more secure have been analyzed.

This thesis has been completed in 2007 and consist of 99 pages.

Keywords : WEP, WAP, WAP2, IEEE 802.11, IEEE 802.1X, TKIP, management keys, integrity, authentication, privacy

TEŞEKKÜR

Çalışmalarım boyunca değerli fikir ve katkılarıyla beni yönlendiren tez danışmanım Prof. Dr. İlhami Yavuz'a, en çok ilgiye ihtiyacı olduğu günlerde kendisine ayırmam gereken zamanlardan çaldığım oğlum Çınar Ulucan'a ve üzerimde hakkı ve emeği geçen herkese teşekkürü bir borç bilirim.

İÇİNDEKİLER

Sayfa

KISALTMALAR

Kısaltma	İngilizcesi	Türkçesi
2G	2. kuşak	2nd generation
3G	3. Kuşak	3th generations
AES	Advanced Encryption Standard	Gelişmiş Şifreleme Standardı
AP	Access Point	Erişim Noktası
bps	Bit per second	Saniyede gönderilen bit sayısı
BSS	Basic Service Set	Temel Servis Set
CCMP	Counter Mode with CBC-MAC Protocol	Sayaç Modlu CBC-MAC Protokolü
CDMA	Code Division Multiple Access	Kod Bölmeli Çoklu Erişim
CDPD	Cellular Digital Packet Data	Hücresel Dijital Paket Veri
DSSS	Direct Sequence Spread Spectrum	Doğrudan Sıralı Yayılım
EAP	Extensible Authentication Protocol	Genişletilebilir Kimlik Doğrulama Protokolü
ESS	Extended Service Set	Genişletilmiş servis seti
ETSI	European Telecomunications Institute	Avrupa Telekomünikasyon Enstitüsü
FCC	Federal Communications Commision	Federal İletişim Komisyonu
FHSS	Frequency Hopping Spread Spectrum	Frekans Atlamalı Yayılım
GHz	Giga Hertz	Giga Hertz

GSM	Global System for Mobile Communications	Mobil İletişimde Global Sistem
HR-DSSS	High Rate Direct Sequence Spread Spectrum	Yüksek Oranlı Doğrudan Sıralı Yayılım
Hz	Hertz	Hertz
ICV	Integrity Check Value	Bütünlük Kontrol Değeri
IEEE	The Institute of Electrical and Electronics Engineers	Elektirik ve Elektronik Enstitüsü
IPSEC	Internet Protocol Security	İnternet Güvenlik Protokolü
ISM	Industrial Scientific Medical	Endüstri Bilim Sağlık
ITU	International Telecommunication Union	Uluslararası Telekominikasyon Birliği
LAN	Local Area Network	Yerel Alan Ağı
LMDS	Local Multiple Distribution Service	Yerel Çok Noktadan Dağıtım Hizmetleri
MAC	Media Access Control	Ortam Erişim Kontrol
Mb	Mega bit	Mega bit
Mbps	Mega bit per second	Saniyede gönderilen megabit sayısı
MHz	Mega Hertz	Mega Hertz
MIC	Message Integrity Code	Mesaj Bütünlük Kodu
MMAC	Multimedia Mobil Access Communication	Çoklu Ortam Mobil Haberleşme
MMDS	Multiple Channel Multiple Distribution Service	Çok Kanallı Çok Noktadan Dağıtım Hizmeti

NIC	Network Interface Card	Ağ Arabirim Kartı
OFDM	Orthogonal Frequency Division Multiplexing	Dikgensel Frekans Bölüşümlü Çoğullama
OSI	Open System Interconnection	Açık Sistem Mimarisi
PAP	Password Authentication Protocol	Şifre Kullanımlı Asıllama Protokolü
PCMCI	Personel Computer Memor**y Card** International Association	Uluslararası Kişisel Bilgisayar Hafıza Kartı Birimi
PDA	Personal Digital Assistant	Kişisel Dijital Asistan
POS	Personal operating system	Kişisel İşletim Sistemi
RADIUS	Remote Authentication Dial-In User Service	Kimlik Asıllama Sunucusu
RAS	Remote Access Server	Uzaktan Erişim Sunucusu
RSN	Robust Security Network	Çok Güvenli Ağ
SIG	Special Interest Group	Özel İlgi Grubu
SNR	Signal to Noise Ratio	Sinyal Gücünün Gürültü gücüne oranı
TKIP	Temporal Key Integrity Protocol	Geçici Anahtar Bütünlük Protokolü
USB	Universal Serial Bus	Evrensel Seri Veriyolu
WEP	Wired Equivalent Privacy	Kabloya Eş Güvenlik
WLAN	Wireless Local Area Network	Kablosuz Yerel Alan Ağı
WMAN	Wireless Metropolitan Area Network	Kişisel Anakent Alan Ağları
WPA	Wi-Fi Protected Access	Wi-Fi Korumalı Erişim

WPA	Wi-Fi Protected Access	Wi-Fi Korumalı Erişim
WPAN	Wireless Personel Area Network	Kablosuz Kişisel Alan Ağları
WWAN	Wireless Wide Area Network	Kablosuz Geniş Ala Ağları

ŞEKİLLER

1. GİRİŞ

Kablosuz teknoloji, bir yada birden fazla aygıtı herhangi bir fiziksel bağlantı olmadan radyo frekansları kullanarak birbirine bağlar. Kablosuz teknoloji dendiğinde akla kablosuz yerel alan ağlardan (WLAN), en basit olarak kulaklıklara kadar pek çok kullanım alanı gelir. Genelde kablosuz ağlarda kullanılan aygıtlar, dizüstü ve taşınabilir bilgisayar, masaüstü bilgisayarı, el bilgisayarı, kişisel dijital yardımcı (PDA), cep telefonu, çağrı cihazlarını, kulaklık, hoparlör, mikrofonu kapsamaktadır. Kablosuz teknolojiler birçok kolaylık sağlar. Örneğin kablosuz teknoloji ile cep telefonundan e-postalara erişilebilmekte, dizüstü bilgisayarlarla hava alanlarında, tren istasyonlarında ve halka açık bazı genel alanlarda Internet'e bağlanılabilmektedir.

WLAN serbest dolaşıma izin vermekte aynı zamanda ucuz ve yüksek bant genişliği servisini de sağlamaktadır. Kablolu bir ağ tasarlamak için ortaya çıkan maliyet ile kablosuz ağ tasarlandığında arada çok fazla bir fark olmadığı görülecektir. Dinamik iş yaşantısının getirdiği yoğun çalışma ortamı, çalışanların ofise bağlı olmadan kaynak paylaşımı, internet erişimi gibi servislerden yararlanma gereksinimini ortaya çıkarmıştır. Bunların sonucunda da kablosuz yerel alan ağları ofis, havaalanı, hastane, istasyon ve topluma açık benzer alanlarda gittikçe daha yaygın kullanılmaya başlanmıştır.

Kablosuz Yerel Alan Ağlarının yararlarını dört ana madde altında toplayabiliriz.

Kullanıcılar için hareketlilik: Kullanıcılar herhangi bir fiziksel bağlantıya kabloya gerek duymadan ağ kaynaklarını kullanabilmektedirler. Aynı zamanda kullanıcılar yüksek hızda ve gerçek zamanda tüm yerel alan ağ (LAN) kaynaklarına mobil olarak erişebilmektedirler.

Hızlı Kurulum: herhangi bir kablolamaya gerek olmadığından, duvarlardan yada yerden kablo çekme, kablolama planında değişiklik yapma gibi işlerle zaman harcanmaz.

Esneklik: Kurulum ve kullanımda esneklik sağlamaktadır. Örneğin kullanıcılar herhangi bir konferans yada toplantı gibi geçici durumlar için kolaylıkla ve hızlı bir şekilde kablosuz yerel alan ağı (WLAN) kurabilirler.

Ölçeklenirlik : WLAN ağ topolojileri, özel uygulama ve kurulum ihtiyaçlarını karşılamak için kolayca konfigüre edilebilir ve küçük eşten eşe ağlardan çok büyük ağlara kadar geniş bir alanda dolaşımı sağlayacak şekilde ölçeklendirilebilir.

Bu temel yararlardan dolayı, WLAN teknolojisi günümüzde hızlı bir şekilde ilerlemektedir. WLAN sistemler artık geleneksel kablolu ağlara bir alternatif olarak karşımıza çıkmaktadır. Örneğin, hastaneler, üniversitelerin birçoğu, havaalanları artık bu hizmeti başlamışlardır.

Kablosuz yerel ağ sistemleri için pek çok farklı standart bulunmaktadır ve geliştirilmektedir. Kullanım amaçlarına, ihtiyaca ve verinin taşınacağı mesafeye göre farklı frekanslar ve standartlar kullanılmaktadır. Geliştirilen yeni teknolojilerin birbirinin yerini alması yerine birlikte kullanılabilmesi ve bu konuda oluşabilecek sorunları önlemek için standartlar yayınlanmaktadır.

Dünyada standartların oluşturulması ile ilgili çeşitli kuruluşlar çalışmalar yürütmektedir. Bu kuruluşlar sistemlerin tanıtımı, cihazların uyumluluk onayları, erişim alanları, sağlanması gereken servisler, güvenlik ilkeleri gibi pek çok konuda bilgi sağlamakta ve yayınlamaktadır.

Kablosuz yerel alan ağları ile ilgili standartları IEEE (Institute of Electrical and Electronics Engineers – Elektrik ve Elektronik Mühendisleri Enstitüsü), ETSI (European Telecomunications Institute – Avrupa Telekomünikasyon Enstitüsü), MMAC (Multimedia Mobil Access Communication – Çoklu Ortam Mobil Haberleşme) olmak üzere üç temel kuruluş tarafından yürütülmektedir.

Bu tezde 802.11 WLAN (Wireless Local Area Network – Kablosuz Yerel Alan Ağları) standartları ve güvenliği incelenmiştir. 802.11 kablosuz ağların güvenliğin artırılması için alınacak önlemler belirtilmiştir.

İkinci bölümde, kapsama alanına göre kablosuz ağ türleri incelenmiş, 802.11 standartları, ve bu standardın fiziksel katmanında kullanılan modülasyon teknikleri ve veri bağlantı katmanı açıklanmıştır.

Üçüncü bölümde, bu tezin asıl konusu olan WLAN kablosuz yerel alan ağlarının çalışma modları, kablosuz ağ bileşenleri ve kablosuz ağ alanı incelenmiştir.

Dördüncü bölümde, WLAN sistemlerde güvenlik unsurları, güvenlik protokolleri, 802.11 standardının güvenlik açıkları belirtilmiştir.

Beşinci Bölümde WLAN sistemlerdeki güvenlik açıklarına karşı alınabilecek önlemler belirtilmiş ve bu sistemi kullanacaklara önerilerde bulunulmuştur.

Altıncı bölümde ise, kablosuz yerel alan ağlarında güvenlikle ilgili değerlendirmeler yapılmıştır.

2. KAPSAMA ALANINA GÖRE KABLOSUZ AĞLAR

Kablosuz ağlar, kablosuz cihazlar arasında yada kablosuz cihazlarla geleneksel kablolu ağlar arasında iletişimi sağlar. Kablosuz ağlar çok çeşitli olmalarına rağmen, genellikle verinin aktarıldığı uzaklığa yani kapsama alanlarına bağlı olarak üç farklı kategoriye ayrılırlar. Kablosuz yerel alan ağları (WLAN), kablosuz geniş alan ağları (WWAN), kablosuz anakent alanı ağları (WMAN), kablosuz kişisel alan ağları (WPAN).

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

En basit şekilde WLAN sistemi bir kablosuz LAN olarak tanımlanabilir. WLAN teknolojileri, kullanıcıların bir alan içinde örneğin, bir üniversite kampüsü, istasyon, havaalanı yada bir şirkette kablosuz bağlantı kurmalarına olanak sağlar. WLAN sistemler, LAN ağlara destek olarak da kullanılabilir. Örneğin, kablolamanın zor olduğu mekanlarda yada kullanıcıların ofis içinde farklı yerlerde ve farklı zamanlarda çalışabilmelerinin gerektiği durumlarda çalışan LAN ağını tamamlamak için kullanılabilirler. WLAN sistemleri lokal (yerel) kullanım amacıyla tasarlandıklarından mesafesi 25-100 metre aralığındadır. [21]

WLAN'ler iki farklı yöntemle çalıştırılabilir. Bunlardan Altyapı (Infrastructure) WLAN sistemlerinde, istasyonlarla varolan ağ omurgası arasında köprü görevini yerine getiren kablosuz erişim noktaları bulunur. Kablosuz istasyonlar bu erişim noktalarına bağlanırlar. Kablosuz erişim noktaları, kablosuz ağ adaptörü olan aygıtlarla iletişim kurar ve RJ-45 portu üzerinden Ethernet LAN sisteme bağlıdır. Genel olarak erişim noktaları yaklaşık 100 metre kapsama alanına sahiptir. Bu alana “hücre” denir. Kullanıcılar dizüstü bilgisayarlarla yada kullanılan diğer kablosuz ağ aygıtlarıyla hücre içinde serbestçe dolaşabilirler. Erişim noktalarının hücreleri birbirlerine bağlanarak kullanıcıların binanın içinde yada binalar arasında dolanımına izin verilir.

Eşler arası sistemler, kablosuz cihazların dinamik olarak birbirlerine bağlanmasını sağlar. Cep telefonları, dizüstü bilgisayarlar yada PDA cihazlarının Bluetooth teknolojisi ile birbirlerine bağlanmasını örnek olarak verebiliriz. Bu sistem, kayan ağ topolojisinden dolayı ad-hoc ismini almıştır. WLAN sistemler sabit bir ağ altyapısı kullanırken, eşler arası sistemler aygıtların birbirleri ile haberleşmelerini sağlayan ve kablosuz linklerle bağlı geçici bir ağ altyapısı kullanır. Bluetooth ağlarda, şebekenin masterı, değişen ağ topolojisini kontrol eder. Ayrıca birbiriyle direk erişim kurma yeteneğine sahip cihazlar arasında akan verinin kontrolünü sağlar. Cihazlar sürekli hareket içerisinde bulunduğundan, dinamik ağ topolojisinden dolayı bu ağlar tekrar tekrar konfigüre edilirler.

Sonuç olarak, eşler arası yani Ad-hoc mod, iki kablosuz ağ cihazının arada başka bir birleştiriciye yani erişim noktasına ihtiyaç duymadan haberleşebildiği durumdur. Eşler arası ad-hoc (özel) sistemler konferans salonu gibi sınırlı bir bölgenin içindeki çok sayıda kullanıcı erişim noktası kullanmadan aralarında geçici bir ağ oluşturabilirler.

WLAN sistemlerinin kullanımı standartlaşmaya bağlı olarak artmaktadır. IEEE 1997 yılında WLAN'ler için saniyede 1 - 2 megabit (Mb) veri aktarım oranını belirleyen 802.11 standardını onaylamıştır. Yaygınlaşan yeni standart olan 802.11b standardında, veriler 2.4 GHz frekans bandı üzerinden en çok 11 Mbps hızında aktarılır. Diğer bir standart 802.11a, 5 GHz frekans bandı üzerinden en çok 54 Mbps hızında veri aktarımı sağlar. Eşler Arası (AD-Hoc) sistemler ise Bluetooth standartlarına dayalı olarak gelişmektedir.

2.2. Kablosuz Geniş Alan Ağları (WWAN – Wireless Wide Area Networking)

WWAN teknolojileri, kullanıcıların, uzak mesafelerde kablosuz bağlantı kurmalarına olanak tanır. Bu bağlantılar uydu yada telsiz üzerinden yapılabilir. WWAN sistemler, kablosuz hizmet sağlayıcılarının sunduğu birden çok anten istasyonu ve uydu sistemi kullanımı aracılığıyla, çok sayıda şehri ve ülkeyi içine

alacak şekilde büyük alanları kapsayabilir. WWAN teknolojileri, ikinci kuşak (2G) sistemler olarak tanınmaktadır. Temel 2G sistemleri, GSM (Global System for Mobile Communications- Mobil İletişimde Global Sistem), CDPD (Cellular Digital Packet Data) ve CDMA (Code Division Multiple Access – Kod Bölmeli Çoklu Erişim) sistemlerini kapsamaktadır. Çalışmalar, içlerinden bazılarının gezici kapasitesi sınırlı olduğundan ve birbirleriyle uyum sağlayamadığından, 2G ağlarından, küresel standarda uygun düşecek ve dünya çapında gezici kapasitesi sağlayacak üçüncü kuşak (3G) teknolojilerine geçiş yapma yolundadır. ITU, 3G için küresel standart geliştirmeyi etkin olarak desteklemektedir. Dünyada birçok ülke bu standardı kullanmaya başlamıştır.[21]

2.3. Kablosuz Anakent Alanı Ağları (WMAN - Wireless Metropolitan Area Networks)

WMAN teknolojileri, kullanıcılara örneğin bir şehir içinde çeşitli yerler arasında kablosuz bağlantılar kurma olanağı verir. Örneğin, bir üniversitenin birbirinden uzak kampüsleri arasında yada birçok yerde ofisi yada şubesi olan şirketler arasında WMAN sistemler kullanılmaktadır. Buna ek olarak, WMAN sistemler, kablolu ağların birincil kiralanmış hatları kullanılabilir olmadığında yedek olarak da hizmet verebilir. WMAN sistemler veri aktarımı için, fiber, bakır yada kiralanmış hatlar yerine, radyo dalgaları veya kızılötesi ışınlar kullanır. Kullanıcıların internete yüksek hızla erişmesini sağlayan geniş bant kablosuz erişim ağlarına talep gittikçe artmaktadır. MMDS (çok kanallı çok noktadan dağıtım hizmeti) ve LMDS (yerel çok noktadan dağıtım hizmetleri) gibi farklı teknolojiler kullanılsa da, geniş bant kablosuz erişim standartlarının IEEE 802.16 çalışma grubu, bu teknolojilerin geliştirilmesini standartlaştırmak için çalışmalarını sürdürmektedir. Bir WMAN 100km erişim mesafesine sahip olabilir. [21]

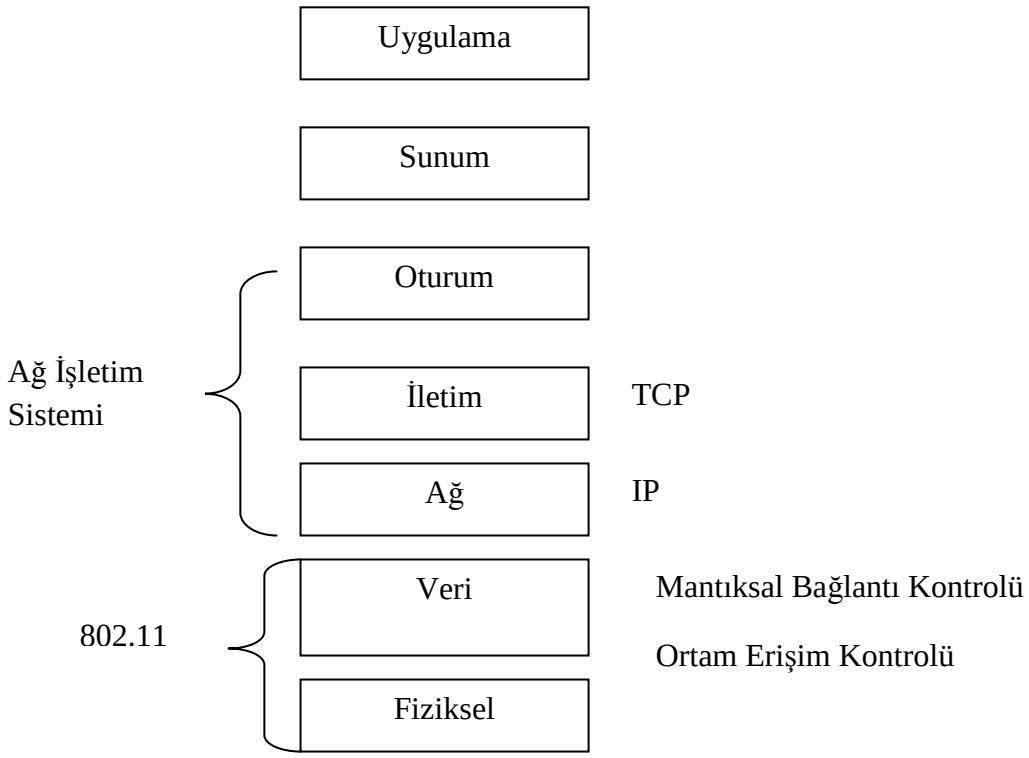
2.4. Kablosuz Kişisel Alan Ağları (WPAN-Wireless Personel Area Networking)

WPAN teknolojileri, kullanıcılara kişisel işletim alanı (POS-Personal Operating System – Kişisel İşletim Sistemi) içinde kullanılacak (aygıtlar için özel, kablosuz iletişim kurma olanağı tanır. Burada sözü geçen cihazlara PDA, cep telefonu veya dizüstü bilgisayarlar örnek verilebilir. Kişisel işletim alanı, kişiyi 10 metre uzaklığa kadar çevreleyen bir alandır. Günümüzde kullanılan iki temel WPAN teknolojisi Bluetooth ve kızılötesi ışındır. Bluetooth, 10 metrelik uzaklığa kadar veri aktarmak için kablo yerine radyo dalgaları kullanan bir teknolojidir. Bluetooth verisi duvar, cep ve evrak çantası içinden geçerek aktarılabilir. Bluetooth teknoloji geliştirme çabaları, 1999'da Bluetooth sürüm 1.0 belirtimlerini yayınlamış Bluetooth Special Interest Group (SIG) tarafından yürütülmektedir. Bunun yanı sıra, kullanıcılar aygıtlar arasında çok kısa mesafelerde (1 metre veya daha az) bağlantı kurmak için kızılötesi bağlantılar oluşturabilir. WPAN teknolojilerinin geliştirilmesini standartlaştırmak amacıyla IEEE, WPAN sistemler için 802.15 çalışma grubunu kurmuştur. Bu çalışma grubu, Bluetooth sürüm 1.0 belirtimine dayanarak bir WPAN standardı geliştirmektedir. Bu taslak standardının ana hedefleri daha az karmaşıklık, düşük güç tüketimi, birlikte çalışabilirlik ve 802.11 ağlarıyla birlikte uyumluluktur. WPAN sistemlere, PDA cihazlarla masaüstü bilgisayarların senkronizasyon işlemi örnek olarak verilebilir. Yada Bluetooth bir kulaklıkla dizüsüstü bir bilgisayardan müzik dinlemek de örnek verilebilir.

2.5. IEEE 802.X Standardı

IEEE (The Institute of Electrical and Electronics Engineers) 802.X adı altında; Yerel ağlar (LAN - Local Area Networks), Metropol ağlar (MAN - Metropolitan Area Networks) ve BlueTooth gibi kişisel ağlar (PAN - Personel Area Networks) için standartlar çıkartmıştır. IEEE'nin 802 standartları, OSI modelinin son

iki katmanı Veri Bağlantı Katmanı (Data Link Layer) ve Fiziksel Katmandaki (Physical Layer) süreç standartlarını ve işlemleri sınırlandırmıştır. [9]



Şekil 2.1. 802.11 ve OSI Modeli [9]

Şekil 2.1'de 802.11 standardının OSI modeli gösterilmiştir.

IEEE 802 LAN/MAN/PAN standartları komitesi kendi içinde 802.1' den 802.17' ye kadar çalışma gruplarına ayrılmıştır.

Bu tanım içindeki en önemli çalışma grupları şunlardır :

802.1: Güvenlik ve diğer konular

802.2: Mantıksal Bağlantı Kontrolleri (LLC - Logical Link Control)

802.11: WLAN sistemler için standartlar üretmek (Kablosuz lokal ağlar)

802.15: WPAN sistemler için standartlar üretmek (Kablosuz kişisel ağlar)

2.6. 802.11 Standartları

Kablosuz yerel ağları için şu anda kullanılan ana standart IEEE 802.11'dir. Sistemde lisanssız ISM bandından 2,4 GHz bandı kullanılmaktadır. IEEE 802.11 ilk olarak 1999' da yayınlanmıştır ve 2.4 GHz band genişliğinde, 2Mbps hızında veri iletişimi için tasarlanmıştır. Bluetooth sisteminde de aynı bant genişliği kullanılmaktadır. Ancak mikrodalga fırınlar gibi araçlarda da aynı bant genişliği kullanıldığından, çeşitli arızalarla karşılaşılması olasıdır. IEEE 802.11 çalışma grupları, bu standardı geliştirmekte ve yeni standartlar "a" harfinden "i" harfine kadar yeniden adlandırılarak yayınlanmaktadır. IEEE 802.11'den sonra ilk çıkan standart 802.11b'dir. Daha sonra 802.11a geliştirilmiştir. Bu iki standardın amacı, bant genişliklerini yükseltmektir. Ancak her ikisi de farklı amaca hizmet etmişlerdir. 802.11a, daha yüksek bant genişliklerinin elde edildiği 5 GHz bandına sapmıştır. Buna karşılık 802.11b ise, 802.11 standardına uyumlu bir gelişim sunmaktadır. 802.11b ile gerçekleştirilen transferler 11 Mbps gibi bir hıza ulaşmaktadır. [1]

802.11 sistemi, diğer sistemlerden daha çok rağbet görmüştür. Yüksek aktarım hızı nedeniyle bu standart daha iyi bir parazit önleme oranına (Signal to Noise Ratio / SNR) ihtiyaç duyar. Sonuç olarak sistemin etkilenme hassasiyeti artar ve diğer sistemlere oranla menzili düşer. IEEE 802.11 sisteminin kapalı alanlarda menzili 30 metre, açık alanlarda ise 300 metredir.

2.7. IEEE 802.11 Fiziksel Katmanı

802.11 standardı fiziksel katmanda tanımı lisans gerektirmeyen üç ayrı kablosuz yöntemi kullanır. Bu yöntemlerden ikisi radyo frekansını biri kızılötesi ışığı kullanır. Kızılötesi sınırlı bir teknolojidir ve çok kısa mesafelerde işletilebilmektedir.

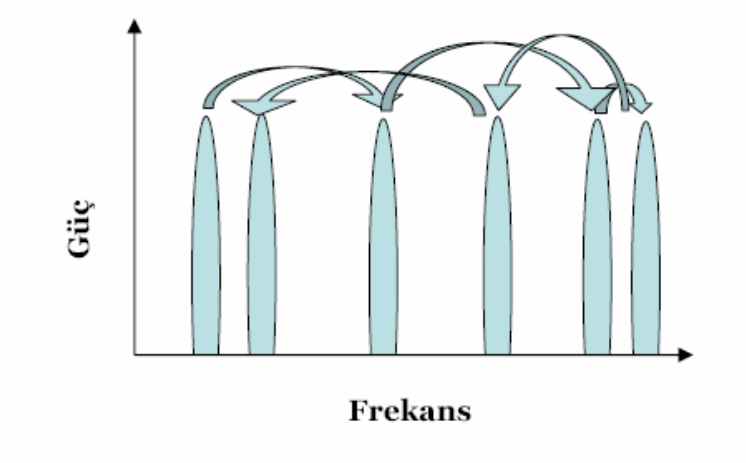
Radyo frekansını kullanan diğer iki teknoloji ise FHSS (Frekans Atlamalı Yayılım - Frequency Hopping Spread Spectrum) ve DSSS (Doğrudan Sıralı Yayılım - Direct Sequence Spread Spectrum) olarak adlandırılan ve etkilenme hassasiyetini düşürmek için fiziksel katmanda kullanılan mekanizmalardır. [5]

Kablosuz yerel ağ standartlarını modülasyon tekniği belirlemektedir. 802.11' in fiziksel katmanında (Physical layer) etkilenme hassasiyetini düşürmek için kullanılan bu iki mekanizmanın yanı sıra daha sonra yüksek band genişliklerine erişmek için geliştirilmiş olan 802.11a ve 802.11b OFDM (Dikgensel Frekans Bölüşümlü Çoğullama - Orthogonal Frequency Division Multiplexing) ve HR-DSSS (High Rate Direct Sequence Spread Spectrum-Yüksek Oranlı Doğrudan Sıralı Yayılım) modülasyon tekniğini kullanmaktadır. [4]

2.7.1. FHSS (Frequency Hopping Spread Spectrum)

Bu teknik, iletim bandını 1MHz'lik alt katmanlara bölmektedir. Sinyal her kanalda belli zaman aralığında kısa veri paketleri göndererek bir alt kanaldan diğerine atlamaktadır. Atlanacak frekansın sırasını üreten bir rasgele sayı üretici kullanılır. Bütün istasyonlar aynı sayı üreticiden bilgi aldığı sürece zamana göre eş uyumlu çalışacak ve eş zamanlı olarak aynı frekansa atlama yapacaklardır. Her frekansta harcanan zaman dilimi yaşam süresi olarak adlandırılır. Atlamaların hem alıcı hem de gönderici tarafından eş zamanlı yapılmaması durumunda bilgi kayıpları meydana gelecektir. [1]

FHSS' de asıl sinyal bir taşıyıcı sinyal üzerine modüle edilir. Taşıyıcı sinyal belli bir sıraya göre sürekli olarak frekansı değiştirir. FHSS' de 2.4 GHz' lik band 1MHz' lik 75 alt kanala (subchannel) bölünmüştür. Alıcı ve verici aynı atlama noktası (hopping pattern) üzerinde olduğunda veri ardaşık olarak alt kanallar üzerinden gönderilir. Şekil 2.2.'de Frekans Atlamalı İletim gösterilmiştir. 802.11'deki her konuşma ayrı atlama noktaları (hopping pattern) üzerinde gerçekleşir ve atlama noktaları, iki göndericinin aynı anda aynı alt kanalı kullanma olasılıklarını en aza indirecek şekilde dizayn edilmiştir. [5]



Şekil 2.2. Frekans Atlamalı İletim [5]

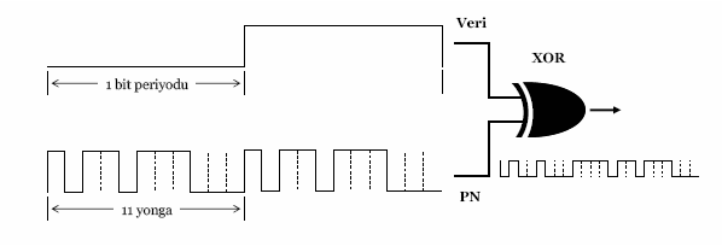
Sonuç olarak FHSS cihazları, belirli bir zaman aralığında kullanılan kanalda, sıradaki bir sonraki kanala atlama gerçekleştirilmeden önce verinin küçük bir miktarının iletilmesi ile sınırlandırılmıştır.

Frekans atlama, frekansın sabit olarak kayması nedeniyle parazite karşı daha az hassasiyet göstermektedir. Bu sayede frekans atlamalı sistemlerin kesintiye uğraması zor olup yüksek güvenlik sağlamaktadır. Frekans atlamalı bir sistemdeki bilgiyi ele geçirmek için tüm bant genişliğine bakmak gerektiğinden, bu sistem askeri alanlarda kullanışlı hale gelmiştir. [5]

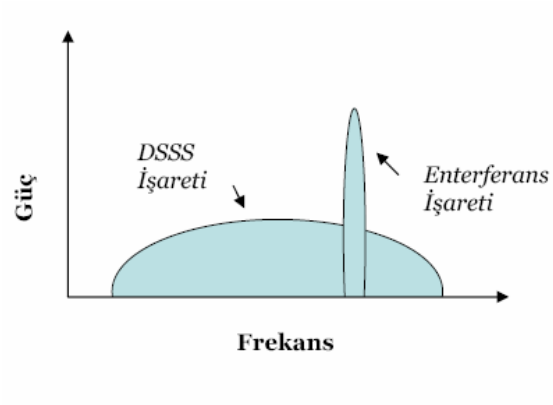
Sinyallerin duvar vb. engellerden yansıyarak alıcı tarafa farklı zamanlarda ulaşmalarından kaynaklanan bozulmalara çoklu yol etkisi denmektedir. FHSS frekans atlamalı bir yapıya sahip olduğu için bu bozulma bir sorun teşkil etmemektedir. Diğer sistemler bu soruna çözüm olarak çeşitli algoritmalar kullanmaktadırlar. [1]

FHSS, 802.11’ de tanımlanmasına rağmen, 802.11 grubu ve cihaz üreticileri tarafından pek rağbet görmeyen bir modülasyon yöntemidir. FHSS uyarlamaları, DSSS’e göre daha ucuz olmalarına ve daha düşük güç tüketmelerine rağmen, düşük veri iletim oranı ve iletim mesafesinde işletilebilirler. FHSS ağır enterferans yaşanan ortamlar için daha uygun bir çözümdür.

2.7.2. DSSS (Direct Sequence Spread Spectrum)



Şekil 2.3. PN dizisi ile Sayısal Modülasyon [5]



Şekil 2.4. DSSS iletimde bozucu işaretin etkisi [5]

Doğrudan Sıralı Geniş Yayılım (Direct Sequence Spread Spectrum) en fazla bilinen ve en geniş kullanım alanına sahip yayılım sistemidir. Bu teknik 2.4 GHz' lik bandı, 22 Mhz' lik kanallara böler. Veri herhangi bir şekilde diğer kanallara atlama olmadan 22 MHz' lik kanallar üzerinden gönderilir. DSSS, modüle edilip iletime uygun hale getirilmiş işaretin, sahte gürültü (PN pseudo-noise) adı verilen dijital sinyalle çarpılması ile gerçekleştirilir. Bu mekanizma bütün bant genişliğini kullanılır ve kullanılan bant genişliğini zaman aralıklarına göre parçalara böler. Yani veri işareti dar bir frekans yerine özel bir kodlama yöntemi kullanılarak çok daha geniş bir frekans bandına dağıtılır. Kullanılan kodlama yönteminde (Sahte Gürültü Düzeni - Pseudo Noise PN) her kod bir bit dizisinden oluşur ve veri biti bu kodlarla taşınır. [22] Şekil 2.3'te PN Dizisi ile Sayısal Modülasyon şekil üzerinde gösterilmiştir.

PN dizisi tarafından kullanılan algoritma rasgele gibi numara üretir ve bu veri dizisinden gelen ikilik düzende bilgi ile ikilik düzende bir kodlama işlemi ile birleştirilir. Elde edilen işaret normalde kullanılandan çok daha geniş bir frekans aralığına, düşük bir güç seviyesinde dağıtılır. Bu DSSS işareti ayrıca dahili bir yedekleme mekanizmasına sahiptir. Asıl verinin 10 yedek kopyası da iletilmektedir. Yedeklilik DSSS' in en avantajlı taraflarından biridir. Alıcı taraf aldığı veri dizisini aynı PN koduna göre işleyerek ham veriyi elde eder. [22]

Eğer aynı band üzerinde bozucu bir işaret mevcut ise bu işaret yüksek güçlü bir dar band işareti gibi görünecektir. Kullanılan kodlamadan dolayı geniş frekans aralığındaki rasgele bölgelerden düşük genlikli işaretler bir araya getirildiğinden alıcı tarafta dağıtık işaret toplanırken, bozucu işaretin güç yoğunluğu dağıtılmış olacaktır. Alıcı taraftaki bu işlemde bozucu işaretin güç yoğunluğu %90 oranında azaltılabilir, böylelikle enterferans neredeyse yok edilmiş olacaktır.[22] Şekil 2.4'te DSSS iletimde bozucu işaretin etkisi gösterilmiştir.

DSSS şu anda 802.11 uygulamalarında en yaygın olarak kullanılan modülasyon tekniğidir ve diğer çözüme göre daha yaygın kullanılmaktadır.

HR-DSSS, 2.4 GHz' lik bantta 11Mbps hıza ulaşmak için kullanılan bir tekniktir. Bu teknik 802.11b ile birlikte standartlaştırılmıştır.

2.7.3. OFDM (Orthogonal Frequency Division Multiplexing)

Bu teknikte, faz kaydırma ve genlik kaydırma yöntemi aynı anda özel bir şekilde kullanılmakta olup geniş bant genişlikleri elde edilebilmektedir. OFDM radyo dalgaları üzerinden büyük miktarda veri transferi yapmak için kullanılan bir frekans bölüşümlü çoğullama modülasyon tekniğidir. OFDM radyo sinyalini daha alt küçük sinyallere bölüp aynı anda farklı frekanslardan alıcıya gönderme yöntemi ile çalışır. OFDM sinyal iletiminde meydana gelen çapraz karışmayı azaltan ve çoklu yol gecikme yayılmasına ve kanal gürültüsüne tolerans tanıyan bir yöntemdir. Bu yüzden pek çok kablosuz uygulama için oldukça uygundur. [2]

OFDM tekniği, yüksek bit hızlı bir veri akışını birkaç adet paralel düşük bit hızlı veri akışına bölen ve bu düşük bit hızlı veri akışlarını birkaç taşıyıcıyı modüle etmek için kullanan bir veri iletim tekniğidir [6]. Toplam band genişliğini dar bandlı alt kanallara bölerek, çoklu yol yayılımları yüzünden meydana gelebilecek gecikme yayılımlarını en aza indirebilir. OFDM' in tercih edilme sebeplerinden biri frekans seçici sönümleme yada dar bant girişime karşı direnci artırmasıdır [7]. Ayrıca dikgen alt taşıyıcılar, band genişliğini olabildiğince verimli bir şekilde kullanmaktadırlar. OFDM tekniğinin sağladığı bu avantajların yanında sistem tasarımında dikkate alınmadığında sistemin çalışmasını olumsuz yönde etkileyecek problemler bulunmaktadır. Tek taşıyıcılı bir sistem ile kıyaslandığı zaman OFDM sisteminin en önemli sakıncalarından biri, zaman ve frekans senkronizasyon hatalarına karşı olan hassaslığıdır. Zaman ve frekans hatalarına karşı sistemi korumak ve sistemin verimini artırmak için senkronizasyon işlemine gerek vardır. OFDM sisteminde eğer alıcı ve verici aynı frekansları kullanıyorsa, OFDM alıcısı alt taşıyıcıları demodüle etmeden önce en azından iki senkronizasyon işlemini gerçekleştirmek zorundadır [7]. İlk olarak sembollerin nerede başladığı belirlenmeli ve ikinci olarak ise alınan sinyalin taşıyıcı frekans kaymalarının tam olarak tahmin edilmesi gerekmektedir. Bu zaman ve frekans senkronizasyon hataları düzeltilmediği zaman semboller arası girişim (ISI) ve taşıyıcılar arası girişim (ICI) meydana gelecek ve bunun sonucunda sistem doğru bir şekilde çalışmayacaktır. OFDM sisteminde senkronizasyonu sağlamak için verici tarafta pilot tonlar gönderilerek senkronizasyon işleminin yapılması sağlanır.

Sonuç olarak, OFDM, çok sayıda modüle edilmiş alt taşıyıcı kullanarak veri iletiminin paralel olarak yapıldığı bir tekniktir. Bu alt taşıyıcılar (yada alt kanallar), mevcut band genişliğini böler ve her bir taşıyıcı için yeterli bir şekilde frekans ayrılarak bu alt taşıyıcıların dikgen olması sağlanır. Taşıyıcılar arasındaki dikgenliğin anlamı; her bir taşıyıcının bir sembol periyodu üzerinde tam sayı periyotlara sahip olmasıdır. Bu sayede her bir taşıyıcının spektrumu, sistemdeki diğer taşıyıcıların her birinin merkez frekansında sıfıra sahip olacaktır. Bunun sonucunda taşıyıcılar arasında spektral olarak üst üste binme olmasına rağmen herhangi bir

girişim meydana gelmeyecektir [7]. Taşıyıcılar arasındaki bu ayrıklık teorik olarak minimum olacak ve çok iyi bir şekilde spektral verimlilik sağlanacaktır. OFDM sistemleri, kablosuz ortamlarda genellikle frekans seçimli çoklu yol tarafından oluşturulan semboller arası girişim (ISI) problemine karşı da kullanılan bir tekniktir.

OFDM, giriş verisine ve kullanılan modülasyon işlemine bağlı olarak gereken spektrum seçilerek meydana getirilir. Kanalda meydana gelebilecek bozulmalara karşı kanal kodlaması ve serpiştirme yapılır.

2.8. IEEE 802.11 Veri Bağlantı Katmanı

802.11’ de veri bağlantı katmanı (Data Link Layer) iki alt katmana ayrılır. Bunlar Mantıksal Bağlantı Kontrolü (Logical Link Control) ve Ortam Erişim Kontrolü (Media Access Control) katmanlarıdır. Bunlardan MAC alt katmanı iletişim kanalının nasıl ayrılacağını ve sonraki transferin kimin tarafından yapılacağını belirlerken, LLC alt katmanının görevi farklı protokoller arasındaki değişiklikleri ağ katmanına belli etmemektir. [11]

802.3 Ethernet LAN yapıda CSMA\CD (Collision Detection Multiple Access/Collision Detection) kullanabilmesinin aksine WLAN sistemlerde çakışmanın algılanması mümkün olamadığından dolayı CSMA\CA(Collesion Detection Multiple Access\Collision Avoidance) kullanır. [4]

802.11 ağa erişimi kontrol etmek için CSMA/CA protokolünü kullanır. CSMA/CA birçok aygıttan aynı andaki iletimden doğan çakışmaları en aza indirgeyen (fakat yok edemeyen) bir "konuşmadan önce dinle" "listen before you talk" metodudur. [8]

CSMA/CA sistemde katılımcılar sessizlik periyotlarında konuşur, eğer konuşma var ise susar. Bu 802.11’i kullanan uçların konuşmak istediklerinde tüm bant genişliğini elde tutmaları anlamına gelir. Bununla birlikte ağa yeni düğümler (node) eklendikçe kanalı elde etmek için çekişme artar, önemli bir zaman

konuşmadaki çakışmaları çözmek için harcanır. Bu nedenle bant genişliğini etken kullanımı düşmüş olur. [4]

Geleneksel kablolu eternetlerin aksine, iletim anında WLAN istasyonları çakışmayı saptayamazlar. CSMA\CA, (Collesion Detection Multiple Access\Collision Avoidance) ACK (acknowledge) paketleri kullanarak çakışmaları önler. ACK paketleri verinin karşı tarafa tam olarak gittiğini garantiler. CSMA\CA kısaca şöyle çalışır. İstasyon ortam boş olduğunda veri gönderebilir. Gönderen taraf veriyi gönderdiğinde bir ACK zamanlayıcıyı başlatır.Paket tam olarak iletildiğinde, alıcı istasyon gönderene ACK paketi yollar. Gönderici istasyon ACK paketini zamanında almadıysa herhangi bir çakışmanın meydana geldiğini anlar ve veri ortamın boş olduğu zaman tekrar gönderilir. [8]

Böylece CSMA/CA hava üzerinde paylaşım sunmaktadır. ACK mekanizması enterferansı ve diğer radyo alakalı problemleri kontrol altında tutar.

Diğer MAC katmanı problemi erişim noktasının iki zıt tarafında duran istasyonların, erişim noktası ile haberleşip birbirleri ile haberleşememesinden kaynaklanır. Bu problemi çözmek için 802.11 Request to Send\Clear to Send protokollerini kullanır. Bu özellik kullanıldığında gönderici istasyon RTS gönderir ve erişim noktasının CTS göndermesini bekler. Ağdaki tüm istasyonlar erişim noktasını duyduğunda CTS onların planlanmış iletim için beklemelerine sebep olur ve böylece herhangi bir çarpışma olmadan verinin gönderilmesi ve ACK paketinin gönderene gelmesi sağlanmış olur. [11]

2.9. IEEE 802.11 Standartları

2.9.1. 802.11b

802.11b'nin temel yapısı, özellikleri ve servisleri orjinal 802.11 standardında tanımlanmıştır. 802.11b tanımı, yüksek veri oranı ve daha güçlü bağlantı ile sadece fiziksel katmanda farklılık gösterir. 802.11b fiziksel katmanın 5.5 Mbps ve 11 Mbps

hızlarını desteklemesini standartlaştırmıştır. Bunu başarmak için fiziksel katmanda DSSS teknolojisini kullanır. 802.11b sistemler, 1Mbps ve 2 Mbps DSSS sistemlerle birlikte çalışabildiği halde, 1Mbps ve 2Mbps FHSS sistemlerle birlikte çalışamaz. 802.11b standardı WLAN teknolojileri için ilk yayınlanan standarttır ve bütün dünyada kullanımı hızla yaygınlaşmıştır. [12] 802.11b standardı, 2.4 GHz bandında, 11 Mbps bant genişliği sunan bir teknolojidir. Sahip olduğu 11 kanallı yapıda örtüşmeyen üç kanal bulunmakta bu sebeple üç adet erişim noktası aynı yerde farklı frekanslarda tutularak bant genişliği üç katına çıkarılabilmektedir. [1]

Yüksek band genişliği gerektiren LAN uygulamaları, daha geniş kapsama alanı gerektiren uygulamalar, güvenilirlik gerektiren uygulamalar, dosya eklemeli e-mail alma-gönderme, web tarama ve dosya paylaşımı gibi uygulamalarda Wi-Fi (802.11b) kullanımı daha uygundur. [2]

2.9.2. 802.11a

802.11a standardı, 5 GHz bandında 54 Mbps bant genişliği sunan WLAN teknolojisidir. 802.11a Ortogonal Frekans Bölmeli Çoğullama (OFDM - Orthogonal Frequency- Division Multiplexing) prensibini kullanır. OFDM ile 48'i veri iletimi için 4'ü hata denetimi için kullanılan toplam 52 kanal tanımlanır. Örtüşmeyen kanal sayısı 802.11b'deki 3'e karşılık burada 8'dir. Ancak komşu kanallar arası girişim etkisi nedeniyle bu kanalların tümü kullanılamaz. [12] 802.11a teknolojisi yüksek veri oranı avantajının yanı sıra 5 GHz gibi yüksek frekans bandı kullanır. Daha geniş band daha fazla radyo kanalı demektir. Her radyo kanalı farklı bir ağa karşılık gelir. Bu standardın en büyük dezavantajı 802.11b standart ile direk olarak uyumlu olmamasıdır. Bu iki standardın bir arada kullanılabilmesi için yeni bir köprü cihazı gerekmektedir. Bu standardın diğer bir dezavantajı ülkemizin de aralarında bulunduğu birçok ülkede sivil amaçlar için kullanımı kısıtlanan 5 GHz bandında çalışması nedeniyle kullanılamaz durumda olmasıdır. [1]

5GHz’lik bandın avantajları olduğu gibi dezavantajları da vardır. 5 GHz’ lik yayının duvar ve diğer objelerden geçerken daha fazla yol kaybına uğrar. Bu sorun

erişim noktalarının sayısını artırmakla çözülebilir. 802.11a ve 802.11b standartlarının birlikte çalışamamalarından dolayı IEEE 802.11g standardını geliştirmiştir.

2.9.3. 802.11g

802.11g standardı, 802.11a'yı kullanamadıkları için 802.11b'nin sunduğu 11 Mbps hızı ile yetinmek durumunda kalan ülkelerin bant genişliği ihtiyacını karşılamak üzere her iki teknolojinin elverişli yönlerinin birleştirilmesiyle oluşturulmuş yeni bir teknolojidir. [12] Teknolojik olarak 2.4 GHz bandında çalıştığı için onun özelliklerini taşır ancak toplam 54 Mbps bant genişliği sunar. 802.11b ile 802.11g geriye dönük uyuma sahiptir yani iki teknoloji aynı yerde çalışabilir. Ülkemizde 2004 yılı bağından itibaren 802.11g ürünleri yaygın olarak kullanılmaktadır. [1]

Sonuç olarak kablosuz ağ teknolojileri görüldüğü üzere, ağın ve uygulamaların ihtiyacı doğrultusunda farklı frekanslarda, farklı hızlarda, farklı koşullarda çalışabilecek şekilde esnek bir yapıya sahiptir. Günümüzün geleneksel kablolu ağlarının kullanıldığı her noktada kablosuz ağ teknolojileri de kullanılabilir, kullanıcıların verimliliğinin ve üretkenliğinin arttığı etkin ağlar kurulabilir.

2.9.4. 802.11i

802.11i standardı IEEE tarafından kablosuz ağlardaki güvenlik problemlerine detaylı çözümler üretmesi amacı ile geliştirilmiştir. Güvenlik dendiğinde akla güvenilir bir şifreleme, güvenilir kimlik doğrulama ve veri bütünlüğünün sağlanması gelir. 802.11i, tüm bu problemleri ortadan kaldıracak RSN (Robust Security Network - Çok Güvenli Ağ) yapısını kablosuz ağlara kazandıracak bir standart olarak düşünülmüştür. [2]

802.11i tüm bu hususları güvenilir ve doğru bir şekilde gerçekleştirmek için şifreleme işlemlerini TKIP (Temporal Key Integrity Protocol) ve CCMP (Counter Mode with CBC-MAC Protocol) protokolleri ile gerçekleştirmektedir. Güvenilir bir

kimlik doğrulaması için 802.1x/EAP protokollerini ve veri bütünlüğünü sağlamak için MIC (Michael Message Integrity Check) algoritmasını kullanır.

Sabit anahtar kullanan WEP' in yeterli güvenlik sağlamaması nedeniyle, 802.11'in bir alt seti olan WPA (Wi-Fi Protected Access) geliştirilmiştir. 802.11i standardı periyodik olarak her 10Kb'da bir şifreleme anahtarlarının değiştirilmesini sağlayan TKIP protokolü ile AES (Advanced Encryption Standard – Gelişmiş Şifreleme Standardı) şifrelemeyi de içermektedir. Bu nedenle bu standardın ismi genellikle WPA2 olarak anılmaktadır.

3. KABLOSUZ YEREL ALAN AĞLARI (WLAN)

WLAN teknoloji, FCC' nin (Federal Communications Commision –Federal İletişim Komisyonu) radyo sinyallerinin endüstride kullanıma açmasıyla birlikte 1980'lerin ortalarından itibaren kullanılmaya başlanmıştır. 1980 'lerde ve 1990' lı yılların başlarında çok yavaş bir şekilde ilerlese de günümüzde teknolojinin vazgeçilmezleri arasına girmektedir.

802.11 Kablosuz ağlarının karakteristik özelliklerine bakılacak olursa, fiziksel katmanda DSSS, FHSS ve OFDM ve kızılötesi kullanmaktadır. 2.4 GHz ve 5 GHz bantları arasında hizmet vermektedir. Veri aktarım oranlarına bakıldığında, 1Mbps, 2Mbps, 11 Mbps (802.11b), 54 Mbps (802.11a) şeklindedir. Veri ve ağ güvenliğine bakıldığında, gizlilik, kimlik doğrulama ve bütünsellik için RC4 tabanlı akış şifreleme algoritması kullanmaktadır. İşletim alanı iç mekanlarda 50 metre, dış alanlarda 500 metredir. Ancak bu değerler engeller, kullanılan araçlardan dolayı değişkendir. Olumlu yönü, eternet hızında kablosuz iletişim ayrıca maliyet olarak hızla düşüşe geçmiş bir aşamadadır. Olumsuz tarafı ise sadece kablosuz teknoloji kullanılan ortamlarda zayıf güvenlik ve ayrıca mesafe ve yük arttıkça belirli bir zaman diliminde işlenen veri oranının azalması olarak söylenebilir. [20]

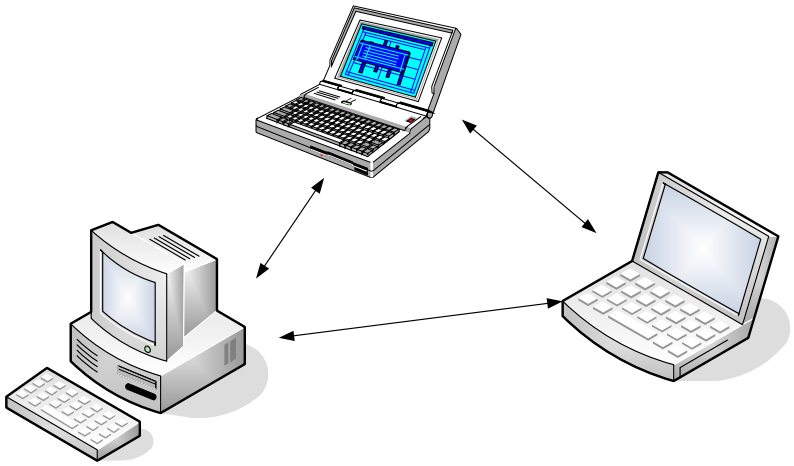
3.1. 802.11'in Yapısı

Kablosuz ağlarda, radyo vericisi ve anten kullanılmaktadır. Kablosuz ağ bileşenleri ise istasyonlar ve erişim noktaları (AP - Access Point) olarak bilinirler.

802.11 standardı, aygıtların direk birbirlerine bağlanmasını sağlayan eşten eşe (peer to peer) ve ağ tabanlı erişim noktalarıyla haberleşmenin sağlandığı iki ayrı yöntem kullanır. Dolayısıyla bu standart iki temel ağ topolojisi tanımlar. Bunlar aygıttan aygıta (ad-hoc, peer-to-peer) ve altyapı (infrastructure) modlarıdır.

3.1.1. Eşler Arası Mod (Ad-Hoc)

Genellikle WLAN sistemler altyapı modunda çalışsalar da eşler arası modda bazı durumlarda kullanılabilmektedir. Eşler arası modda, her kullanıcı ağdaki biri diğeri ile iletişim kurar. [4] Şekil 3.1.'de Eşler Arası Mod gösterilmişitir.



Şekil 3.1. WLAN sistemlerde Eşler Arası Mod (Ad-Hoc) [10]

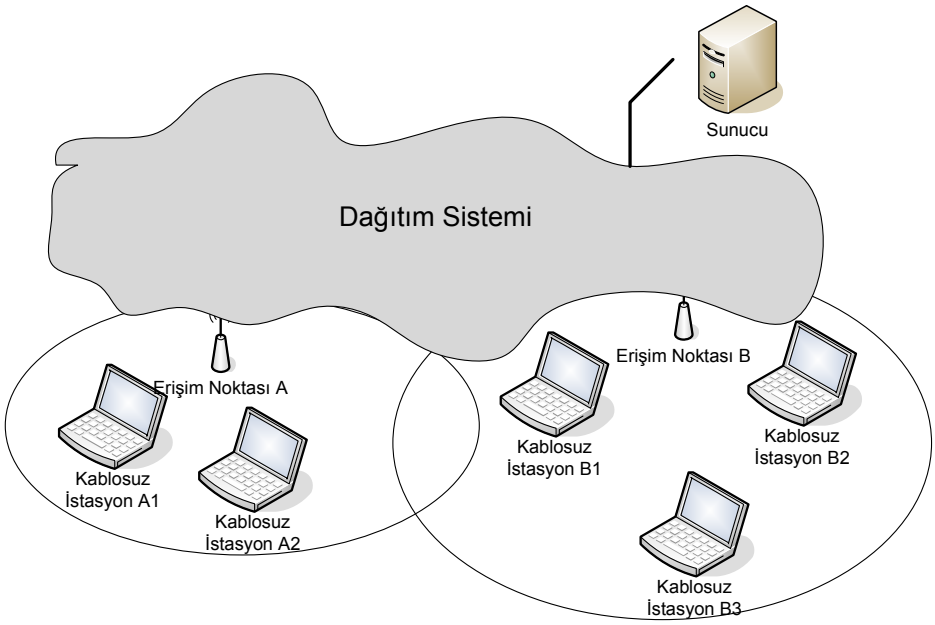
Bu mod, birbirleri ile iletişim mesafesinde olan kullanıcılar için tasarlanmıştır. Örneğin aynı oda içersinde bulunan bilgisayarlar bu topolojiyi kullanarak direk birbirlerine bağlanabilir. Eşler arası topolojide, istasyonlar birbirleriyle makineden makineye iletişim kurduklarından konuşmak için herhangi bir izne gerek yoktur. Eğer bir kullanıcı bu tanımlanmış mesafeden dışarıya çıkarak iletişim kurmak isterse, arada bir kullanıcı ağ geçidi ve yönlendirici olarak görev yapmak zorundadır. Bu yapıda aygıtlar herhangi bir erişim noktası kullanmadan birbirleriyle kaynak paylaşımında bulunabilirler. [1]

3.1.2. Altyapı Modu (Infrastructure)

Altyapı ağları, kablosuz hücrelerle kablolu yerel alan ağların (LAN) alanlarının genişletilmesini sağlar. Bir dizüstü bilgisayar yada başka bir mobil cihaz yerel alan ağ (LAN) kaynaklarına erişime devam ederek bir hücreden diğerine geçebilir. Burada sözü geçen 'hücre' erişim noktasının kapsama alanıdır ve bu alan temel servis set (Basic Service Set-BSS) olarak adlandırılır. Başka bir tanımla iki veya daha fazla istasyon birbirleriyle iletişim için bir araya geldiklerinde Temel Servis Set (Basic Service Set- BSS) oluşturmuş olurlar. Yani temel servis sette iki veya daha fazla istasyon birbirleri ile ve ağ ile iletişim kurarlar. En küçük BBS için iki istasyona ihtiyaç vardır. [20]

BSS' ler bir ağa bağlandığında altyapı mod oluşur. 802.11 yapısı bazı elemanlara sahiptir. İki veya daha fazla BSS, bir dağıtım sistemi (Distribution System-DS) kullanarak birbirlerine bağlanırlar. Bu durum ağın alanını (network coverage) artırır. Böylece her BSS ağın bir parçası haline gelir. DS'ye giriş erişim noktası kullanımı ile yapılır. Veri, BSS ile DS arasında erişim noktası yardımı ile taşınır. Daha açık söylemek gerekirse her istasyon bağlantı isteklerini bağlantı merkezi olarak bilinen erişim noktasına (AP - Access Point) yani merkez istasyona yollar. Erişim noktaları bildiğimiz kablolu ağ anahtarları gibi çalışır ve iletişimi kablolu veya diğer bir kablosuz ağa yönlendirir. [1] Şekil 3.2.'de Altyapı Modu gösterilmiştir.

Bir altyapı ağında, tüm hücrelerin toplamı genişletilmiş servis seti oluşturur. Diğer bir deyişle genişletilmiş servis sette (Extended Service Set - ESS), BBS' ler birbirine bağlanmıştır. Bu yapı genellikle kampüs ve binalar arasında kablosuz ağ olanağı sağlamaktadır. ESS, Mantıksal Bağlantı Katmanında (Logical Link Layer) bağımsız bir BSS olarak görünür. Yani ESS içindeki istasyonlar birbirleriyle iletişim kurabilirler ve hatta hareket edebilirler. [20]



Şekil 3.2. Altyapı Modu [10]

Daha açık bir şekilde anlatmak gerekirse, kablosuz ağlar, erişim noktaları ile iletişim kurabilmek için radyo modemler kullanan istasyonlara sahiptir. İstasyonlarda radyo alıcı vericileri içeren kablosuz arabirim kartları bulunmaktadır. Erişim noktaları ise bir tarafta radyo alıcı vericisi, diğer tarafta ise kablolu omurgaya bağlı bir köprü (bridge) içermektedir. Erişim noktaları, kablolu yapının hareketsiz sabit parçalarından biridir ve hücresel iletişimdeki hücre alanı (cellsite) ile benzeşmektedir. İstasyonlar arasında ve istasyonlarla kablolu ağ arasında kurulacak her türlü iletişim erişim noktaları üzerinden yapılmaktadır.

3.2. Kablosuz Ağ Bileşenleri

WLAN sistemler, kablosuz istasyonlar ve erişim noktaları olmak üzere iki tip bileşen içerirler. Burada sözü geçen istasyon, kablosuz bir ağ arabirim bağdaştırıcısı içeren dizüstü bilgisayar yada masaüstü bilgisayar olabilir. Aynı zamanda bir PDA yada özel bir barkod tarayıcısı da olabilir. Kablosuz dizüstü bilgisayarlar diğer

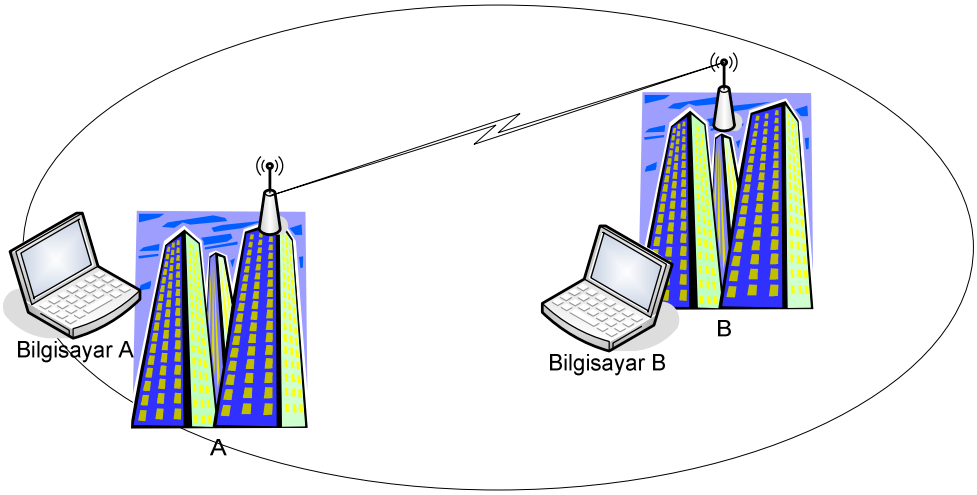
dizüstü bilgisayarlardan farklı olarak erişim noktalarına bağlantı sağlayacak kablosuz arabirim bağdaştırıcısı (NIC Network Interface Card – Ağ Arabirim Kartı) içermektedir. Kablosuz ağ bağdaştırıcısı ayrıca PCMCI (Personel Computer Memory Card International Association) yuvasına veya USB (Universal Serial Bus - Evrensel Seri Veriyolu) portuna dışardan da bağlanabilmektedir.

Kablosuz ağ bağdaştırıcıları WLAN ağı ile bağlantı kurabilmek için radyo sinyalleri kullanır. Kablolu ve kablosuz ağlar arasında köprü görevini yapan erişim noktaları, radyo alıcı ve vericisi, kablolu ağ arabirimi ve köprü görevini yerine getirebilmesi için gerekli yazılımı içermektedir.

3.3. Kablosuz Ağ Alanı

802.11 kablosuz ağlar için güvenli kapsama alanı, çeşitli faktörlere dayanmaktadır. Bunlarda birkaçı, istenen veri iletim oranı ve kapasite, radyo frekans arabirimin kaynakları, fiziksel alan ve karakteristiği, güç, bağlantıda sürereklilik ve kullanılan anten olarak belirtilebilir. Teorik olarak, kapsama alanı kapalı alanlarda 11 Mbps için 29 metreden, açık alanlarda 1 Mbps için 485 metreye kadar çıkmaktadır. Ancak deneysel analizlerde 802.11'in aygıtları kapalı yerlerde yaklaşık 50 metre gibi bir alanda çalıştığı görülmektedir. Ayrıca 400 metre bir çok kampüs uygulaması için WLAN yapının ideal bir teknoloji olduğunu göstermektedir.

Erişim noktaları ayrıca köprü (bridge) görevini yerine getirmektedir. Köprü iki veya daha fazla ağı birbirine bağlamakta ve ağ trafiğini değiş tokuş yaparak onların iletişim kurmalarına izin vermektedir. Köprü noktadan noktaya yada birden çok nokta arasında konfigürasyonu içerebilmektedir. Noktadan noktaya yapıda, iki LAN kendi erişim noktaları üzerinden birbirlerine bağlanırlar. Birden çok nokta arasında köprü yapısında ise, LAN üzerindeki bir altağ (subnet) LAN üzerindeki diğer altağlara her altağdaki erişim noktası aracılığı ile bağlanır. Örneğin A altağındaki bir bilgisayar, B altağında bir bilgisayara bağlanmak istediğinde, A altağının erişim noktası B altağının erişim noktasına bağlanacaktır.



Şekil 3.3. Erişim Noktasının Köprü İşlevi [20]

Bir işyeri kampüsünde bulunan farklı binalar arasındaki yerel alan ağları köprüleme yöntemiyle birbirine bağlanır. Köprü fonksiyonlu erişim noktası cihazları, tipik olarak binaların çatısına yerleştirilmektedir. Her iki köprü erişim noktası arasındaki uzaklık yaklaşık olarak 2 mildir. Bu mesafe birçok faktöre göre de değişiklik gösterebilir. Şekil 3.3'te Erişim noktasının köprü işlevi gösterilmiştir. Şekil 3.3.'te, A bilgisayarından B bilgisayarına gönderilen kablosuz veri, bir binadan diğerine, herbir binanın uygun yerine yerleştirilen erişim noktaları aracılığıyla gönderilir. A bilgisayarı bina içerisinde en yakın erişim noktasına bağlanır. A binasındaki erişim noktası aldığı veriyi binanın çatısında bulunan ve köprü görevini gören erişim noktasına iletir. Bu köprü veriyi yan binadaki köprüye yönlendirir. B binasındaki köprü erişim noktası da veriyi B bilgisayarına gönderir. [20]

4. 802.11 WLAN SİSTEMLERDE GÜVENLİK

IEEE, WLAN sistemler için üç temel güvenlik servisi tanımlamıştır. Bunlar, kimlik doğrulama, gizlilik ve bütünlüktür servisleridir.

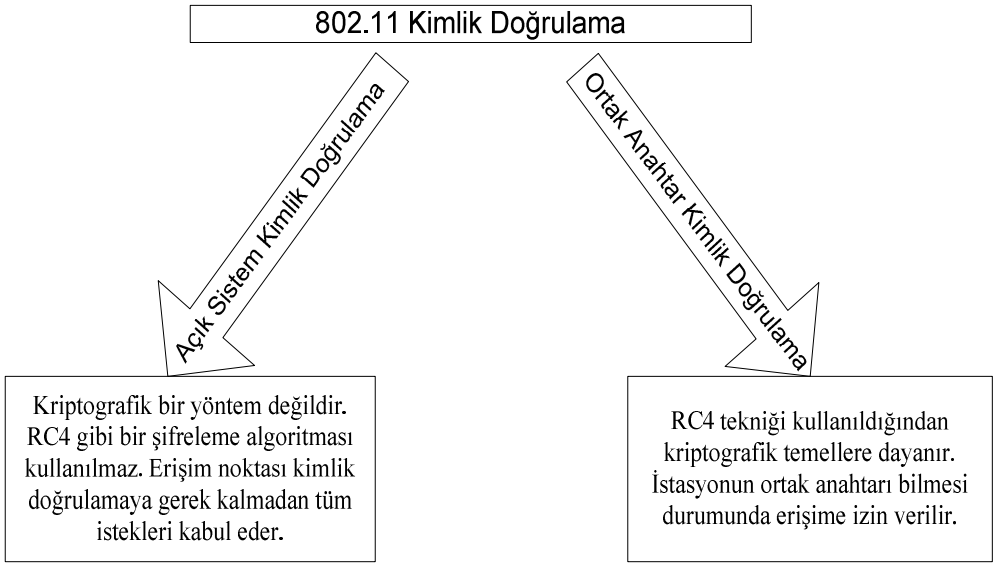
Kimlik Doğrulama: WEP'in birincil amacı, iletişim kuran istasyonların kimliklerini doğrulamak için güvenlik servisi sağlamasıdır. Böylece, kimliği doğrulamayan istasyonların ağa girişini önleyerek ağa erişimi kontrol altına alır. Bu servis, kimliği dorulanmış kişilerin yani ağa giriş yetkisi olan kullanıcıların ağa girişini kontrol eder.

Gizlilik: WEP'in ikinci amacı, pasif atakları önlemektir. Bu servis kasıtlı olmayan hattı dinlemelere yani pasif ataklara karşı ağı korur. Servis, "sadece yetkilendirilmiş kişiler mi ağdaki verilere ulaşıyor" sorusuna cevap verir.

Bütünsellik, Bozulmamışlık: WEP'in diğer bir amacıda, kablosuz istasyondan erişim noktasına kadar mesajın değişmeden ulaşmasını sağlamaktır. Bu servis "ağa gelen yada giden veri güvenilir mi, yoksa yoldan değişikliğe uğramış mı "sorularına cevap verir.

4.1. Kimlik Doğrulama

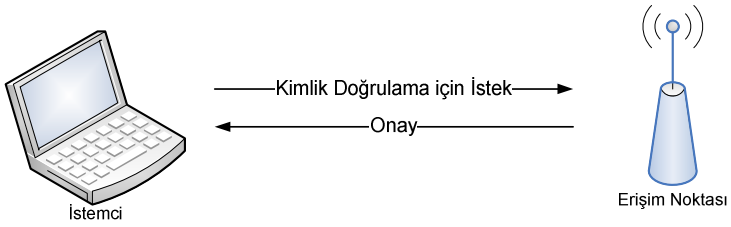
Veri iletişimi başlamadan önce kullanıcılar ve erişim noktaları arasında ilişkilendirme yapılması gereklidir. Bu ilişkilendirme yapılmadan önce kimlik doğrulama işlemi yapılır. Şekil 4.1.'de 802.11 standardında kullanılan Kimlik Doğrulama Teknikleri gösterilmiştir. IEEE 802.11 kablolu ağa erişmek isteyen kullanıcaları iki şekilde doğrular. Bunlar açık sistem ve ortak anahtar yöntemleri ile kimlik doğrulamadır. Ortak anahtar yöntemi kriptografiye dayanırken, açık sistem yönteminde herhangi bir şifreleme kullanılmamaktadır. Erişim noktası istasyonların kimliğinin doğrulanmasına gerek kalmadan tüm istekleri kabul eder. Dolayısıyla açık sistem tekniği bir kimlik doğrulama yöntemi değildir. Aynı zamanda, burada sözü geçen kimlik doğrulama tek yönlüdür. Sadece istasyonun kimliği doğrulanır.



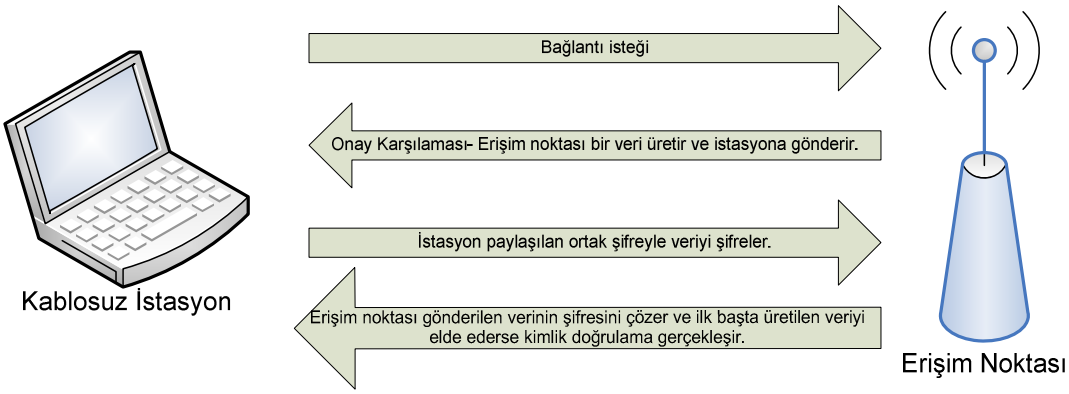
Şekil 4.1. 802.11 standardında Kimlik Doğrulama Teknikleri

Ancak istasyon iletişime geçtiği erişim noktasının gerçek erişim noktası olduğuna güvenmek zorundadır. [1]

Şekil 4.2 ‘de Açık Sistem Kimlik Doğrulama adımları gösterilmiştir. Açık sistem asıllama yönteminde, istasyon ve erişim noktası arasında iki mesaj alışverişi olur. Bu mesajlar sırasında istasyon erişim noktasına MAC adresini gönderdiğinde doğrulama gerçekleşir. Aslında erişim noktası ile istasyon arasında geçen bu iki mesaj sırasında tam bir doğrulama yapılmış olmaz. Çünkü erişim noktasının gönderdiği mesaj içerisindeki doğru alanları yanıtlayan istasyonun kimliği doğrulanmış sayılır. Herhangi bir kriptografik sınama olmadığından da, açık sistem asıllama yönteminin saldırılara çok fazla açık olduğu söylenebilir. [2]



Şekil 4.2. Açık Sistem Asıllama Yöntemi [23]

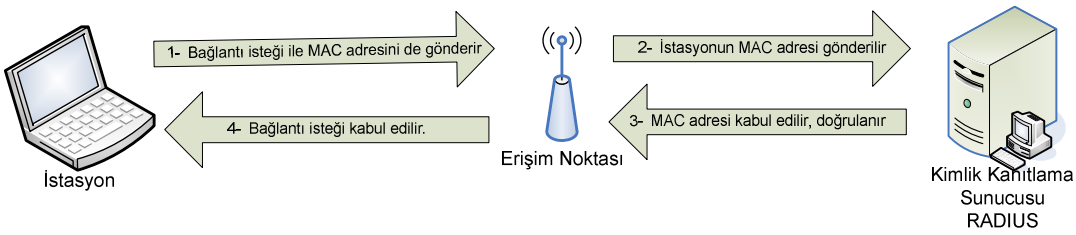


Şekil 4.3. Ortak Anahtar Yöntemi ile Asıllama [23]

Şekil 4.3.'te Ortak Anahtar Yöntemi ile Asıllama gösterilmiştir. Ortak anahtar yönteminde asıllama için kriptografik teknik kullanılmaktadır. Burada erişim noktası tarafından rastgele bir veri (challenge) üretilir ve kablosuz istasyona gönderilir. Erişim noktasıyla paylaşılan anahtar kullanan istasyon, rastgele üretilen veriyi, ortak anahtarla şifreler ve sonucu erişim noktasına gönderir. Erişim noktası, istasyon tarafından işlenen bu sonucun şifresini çözer ve eğer bu değer en başta gönderilen rastgele veriye eşitse erişime izin verir.

Kriptografik hesaplamada ve 128 bitlik rastgele verinin üretilmesinde kullanılan bu algoritma Ron Rivest tarafından geliştirilmiş RC4 şifreli akış (Stream cipher) algoritmasıdır. Ancak burada anlatılan asıllama metodu çok temel ve basit bir kriptografik tekniktir ve karşılıklı bir asıllama sağlamaz. Bu methotda istasyon erişim noktasının kimliğini doğrulamaz. Bu yüzden istasyonun doğru erişim noktası ve kablosuz ağa bağlandığının garantisi yoktur. Tek taraflı kimlik doğrulama şeması zayıf yapıdadır. Yani, ortadaki adam saldırıları (man-in-the- middle) olarak bilinen tarafların haberi olmadan mesajları değiştirebilen ataklara açıktır. [20]

Bu iki asıllama yöntemi dışında MAC adresi kullanarak asıllama da yapılır. Erişim noktası üzerinden haberleşebilecek kullanıcıların MAC (Media Access Control – Ortam Erişim Kontrol) adresleri bir sunucuda (RADIUS - Remote



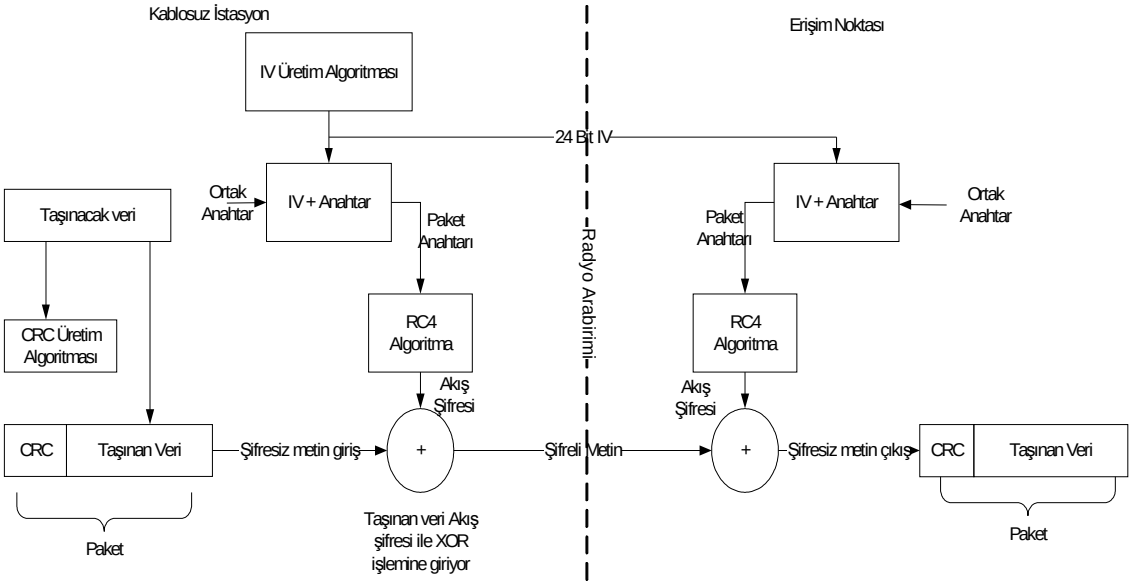
Şekil 4.4. MAC Adresi ile Asıllama [23]

Authentication Dial-In User Service – Kimlik Asıllama Sunucusu) tutularak, sadece önceden belirlenmiş MAC adreslerine sahip kullanıcıların asıllanması sağlanır. Bu sistemin çalışması Şekil 4.4.'te gösterilmiştir.

- Kullanıcı erişim noktasına asıllama isteğini ve MAC adresini gönderir.
- Erişim noktası, kullanıcının MAC adresini RADIUS sunucusuna gönderir.
- Sunucu belirlenen MAC adresleri içinde gönderilen MAC adresinin olup olmadığını kontrol ederek, erişim noktasına sonucu gönderir.
- Erişim noktası gelen bilgiye göre kullanıcıyı asıllar yada reddeder.

4.2. Gizlilik

802.11 standardı, kablosuz arabirimler için kriptografik teknikler kullanarak gizlilik servisini sağlar. WEP kriptolojisi, gizlilik için RC4 simetrik anahtar kullanmaktadır. Bu algortimada, sahte rastgele veri dizisi (pseudo-random data sequence) üretilmektedir. WEP tekniği kullanılarak, kablosuz bağlantı sırasındaki iletimde herhangi bir şekilde verinin ele geçirilmesi önlenmiş olur. WEP, TCP/IP, IPX, HTTP protokollerindeki trafiği korumak için, 802.11 WLAN katmanları üzerindeki tüm veriye uygulanır. Gönderici, bu anahtar veri dizisini göndereceği metin ile XOR işlemine tabi tutar. ("XOR - Exclusive or" - Ayrıcalıklı 'veya') ve şifrelenmiş metni üretir.



Şekil 4.5. RC4 Algoritması Kullanarak WEP Veri Gizliliğinin Sağlanması [20]

802.11'de tanımlandığı üzere, WEP, ortak anahtar için, 40 bit kriptografik anahtar uzunluğunu destekler. Ancak WEP'in 40 bitten 104 bite kadar uzunluğu destekleyen ve standart olmayan değişik uzantıları vardır. 104 bitlik anahtar, 24 bitlik başlangıç vektörü ile, 128 bitlik RC4 anahtarı haline gelir. Genel anlamda diğer özellikler aynıdır, anahtar uzunluğunun artması, kriptografik tekniğin güvenliğini artırır. Yapılan araştırmalar, sağlıklı, güvenilir uygulamalar ve dizaynlar için, 80 bit ve üzeri anahtar uzunluğunun kod kırmayı imkansızlaştırdığını göstermektedir. 80 bitlik anahtar için 10^{26} üzerinde bir anahtar alanından bahsedilir ki bu günümüzün bilgisayarlarının gücünü aşar. Pratikte, genellikle birçok WLAN uygulamasında 40 bitlik anahtar kullanıldığı görülmektedir. Ayrıca geçmişteki saldırılar, WEP'in gizlilik anlamında anahtar uzunluğuna rağmen saldırılara açık olduğunu göstermektedir. [20] Şekil 4.5.'te RC4 Algoritması Kullanarak WEP Veri Gizliliğinin Sağlanması gösterilmiştir.

4.3. Bütünlük

802.11 aynı zamanda erişim noktası ile kablosuz istasyon arasında gelen giden mesajların veri bütünlüğünü de sağlamaktadır. Bu güvenlik servisi, mesajların yolda değiştirilmesini engelleyecek şekilde dizayn edilmiştir. Bu teknik, basit ve şifreli dönüşsel yedeklilik denetimi (Cyclic Redundancy Check – CRC) yaklaşımı kullanır. Şekil 4.5.'te görüldüğü gibi, iletimden önce her veri CRC dizisi ile birleşir. Bu integrity-sealed packet (bütünlüğü sağlanmış- sızdırmaz paket) RC4 algoritması ile şifrelenerek, Cipher text denilen şifreli mesajı oluşturur. Alıcı tarafta, önce şifre çözülür ve ardından alınan mesaj üzerindeki CRC dizisi tekrar hesaplanır. Alıcı taraftaki CRC dizisi orijinal mesajdaki CRC dizisi ile karşılaştırılır. Eğer aynı değillerse paketin yolda değişikliğe uğradığı anlaşılır ve bu paket atılır. 802.11 gizlilik servisi açısından bakıldığında CRC kullanımı nedeniyle saldırılara açıktır. Özet olarak, WEP protolündeki bütünlük şemasında en temel kusur, CRC'nin kriptografik olarak güvenlik mekanizmasına sahip olmamasıdır. [20]

802.11 standardında, malesef anahtar yönetimine dair herhangi bir tanımlama (kriptografik anahtarların yaşam süresi vb) bulunmamaktadır. Bu yüzden, dağıtma, üretme, saklama, yükleme, risklere karşı ektra koruma, güvenlik amaçlı denetim gibi uygulamalar WLAN sistemi kullananlara bırakılmıştır. Anahtar yönetimi bu açıdan bakıldığında 802.11'i kullanacak kişilere bırakılmıştır. Sonuç olarak, WLAN ortamı saldırılara oldukça açık bir yapıdadır. Ürünlerin fabrika çıkışı varsayılan anahtarlarının kullanımına devam edilmesi, anahtarların belirli zaman aralıklarında değiştirilmemesi, tüm karekterleri sıfır yada bir değerlerinden oluşan zayıf anahtar kullanımı, kolay bir şekilde tahmin edilebilecek zayıf anahtar kullanımı ile saldırılara davet çıkarabilmektedir. Ayrıca anahtar yönetimi orjinal 802.11 standardında tanımlanmadığından anahtar dağıtımı belirtilmediğinden WEP güvenlikli WLAN sistemler iyi bir şekilde planlanmamış demektir. Eğer sık sık anahtar değişimine gerek varsa ve bu anahtarlar rastgele değişecekse, büyük WLAN ortamlarına bu iş nerdeyse imkansız hale gelmektedir. Örneğin 20000 erişim noktasının bulunduğu bir WLAN ortamı düşünelim. Böylesine büyük bir alanda anahtar yönetimi, üretimi,

dağıtımı önemli ve zor bir görevdir. Büyük dinamik ağlarda anahtar dağıtımının pratik yolu anahtarların yayınlanması ile mümkün olabilir. [20]

802.11'in kablosuz ağlarda kullanılmak üzere ilk geliştirdiği WEP (Wired Equivalent Privacy- Kabloya Eş Güvenlik) protokolünün ardından WEP'in güvenlik açıklarından dolayı WPA (Wi-Fi Protected Access – Wi-Fi Korumalı Erişim) ve EAP (Extensible Authentication Protocol – Genişletilmiş Kimlik Doğrulama Protkolü) protokolleri geliştirilmiştir.

4.4. WEP (Wired Equivalent Privacy- Kabloya Eş Güvenlik)

802.11 tanımlamalarında güvenli bir işletim alanı sağlamak için pek çok servis belirlenmiştir. Bu güvenlik servislerinin pek çoğu, erişim noktalarıyla istasyonlar arasındaki kablosuz iletişim sırasında bağlantı-düzeyli koruma için kullanılan WEP (Wired Equivalent Privacy – Kabloya Eş Güvenlik) protokolü tarafından sağlanmaktadır. WEP uçtan uca güvenlik sağlamamakla birlikte, sadece kablosuz iletişim kısmında güvenlik sağlamaktadır. [2]

Kablolu ağlardaki eşdeğer protokol veya WEP, yazarları tarafından ilk olarak 802.11 standardı olarak tasarlanmıştır. WEP, IPSEC gibi güvenli bir ağ protokolu olma desteği verecek şekilde tasarlanmamıştır. Fakat eşit seviyede kişisel güvenlik sağlamaktadır. WEP, radyo dalgaları üzerindeki verilerin şifrelenesini sağlamaktadır. WEP, kablosuz ağlara izinsiz girişleri engellemek için kullanılmaktadır. Bu protokol normalde başlangıç değeri olarak kullanımda değildir. Eğer kullanıma açılırsa, gönderilen her paket şifreli olarak iletilecektir. [1]

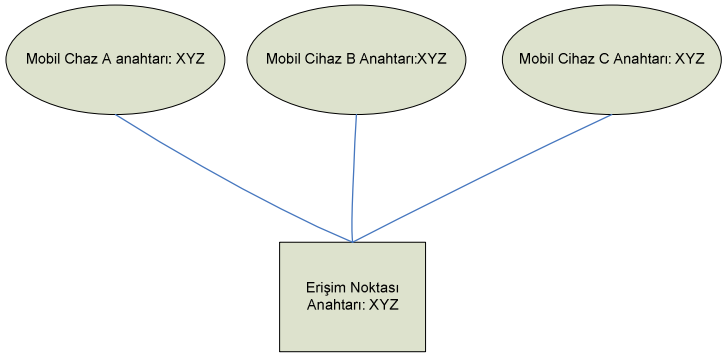
WEP protokolü, temel servis setlerde (Basic Set Service) paylaşılmış olan gizli anahtar mantığına dayalıdır. Bu anahtar, veri paketlerini göndermeden önce şifrelemek ve bunların veri bütünlüğünü kontrol etmek için, paketlerin yolda değiştirilip değiştirilmediği kontrol etmek için kullanılır. WEP, akış (stream) şifreleme olan RC4 algoritmasını kullanır. Akış şifreleme, kısa anahtardan sonsuz

sahte rastgele anahtara (infinite pseudo-random key) genişletilmiştir. Gönderici bu anahtar dizisini göndereceği metin ile XOR işlemine tabi tutar. ("XOR - Exclusive or" - Ayrıcalıklı 'veya') ve şifrelenmiş metni üretir. 2 bit veri XOR fonksiyonuna tabi tutulduğunda 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 işlemine tabi tutulunca orijinal metin elde edilir. [8]

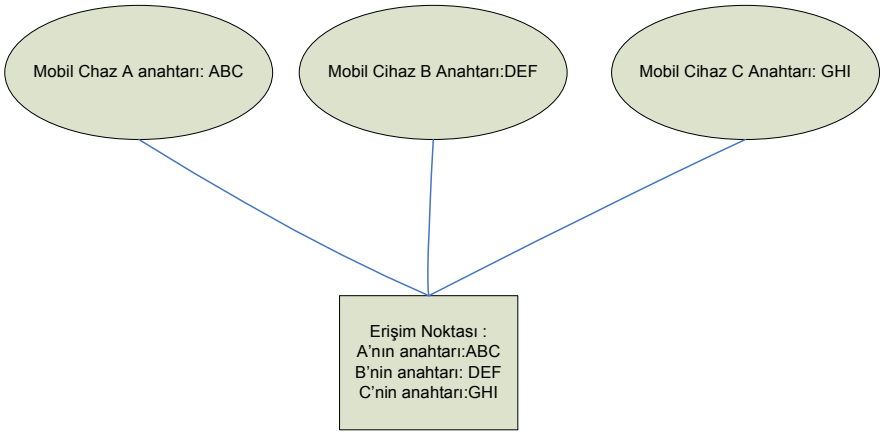
Kullanılan şifreleme algoritması RC4, anahtar uzunluğu 40 bit veya 104 bit, başlangıç vektörü (IV - initialization vector) uzunluğu 24 bit, veri bütünlüğünü bütünlük kontrol değeri (ICV - integrity check value) ile sağlanmaktadır. Kullanılan şifreleme algoritması RC4, simetrik anahtar kullanmaktadır. [20]

WEP'te Kullanılan Anahtarlar :

WEP' te kullanılabilecek anahtarlar iki gruba ayrılır. Bunlar ön seçili anahtarlar ve kullanıcıya özel anahtarlardır. Şekil 4.6.'da ön seçili anahtarlı yapı gösterilmiştir. Ön seçili anahtarlı yapıda erişim noktası ve kullanıcılar veri şifrelemede aynı anahtarı kullanır. Açıkça görüldüğü gibi bu yöntem kullanıldığında tüm kullanıcılar tüm verileri çözebilirler.



Şekil 4.6. WEP protokolünde ön seçili anahtarlar [13]



Şekil 4.7. WEP protokolünde özel anahtar kullanımı [13]

İkinci yöntemde ise erişim noktası her kullanıcıya karşılık farklı anahtarlar bulundurmaktadır. Bu sayede kullanıcı sadece kendine gelen verileri çözme yeteneğine sahip olacaktır. [8] Bu durum Şekil 4.7.'de gösterilmiştir.

WEP şifreleme şu şekilde çalışmaktadır. 24 bitlik başlangıç vektörü (IV-Initialization Vector), 40 bitlik paylaşılan anahtara eklenir. Bu anahtardan RC4 algoritması kullanılarak şifrelenecek veri uzunluğunda akış şifresi elde edilir. IV vektörünün değişmesi ile her seferinde farklı akış şifreleri elde edilmektedir. Bu sırada veri bütünlüğü sağlamak için asıl veri üzerinden ICV hesaplanır ve verinin sonuna eklenir. Elde edilen akış şifresi ile (veri +ICV) dar veya işleminden geçirilerek şifreli metin hazırlanmış olur. Son adım olarak alıcı tarafın şifreyi çözmesi için bilmesi gerekli olan IV çerçevenin başına şifrelenmeden eklenir. Böylelikle gönderilecek çerçeve hazırlanmış olur. [1]

Şifre çözmede ise alıcı taraf başlangıç vektörünü çerçeveden okur. Zaten anahtar kendinde olduğu için akış şifresini elde edebilir. Şifreleme işlemlerini ters sıra ile gerçekleştirerek açık veriyi elde eder.

4.5. WPA (Wi-Fi Protected Access – Wi-Fi Korumalı Erişim)

Güvenlik standartları IEEE grupları tarafından belirlense bile bazı bölümler üretici şirketleri tarafından farklı gerçeklenebilir. Bu farklılığı önlemek ve üretilecek cihazların uyumluluğunu sağlamak için oluşturulan maddi amaç gütmeyen bir ortaklık kurulmuştur. Bu ortaklığın adı Wi-Fi dır.

WEP deki kusurlar 2001 yılından beri açık bir şekilde bilinmektedir. IEEE 802.11' deki sorunları çözecek standartları geliştirmek için çalışmalara başlayarak 802.11i geliştirme çalışmalarına başlamıştır. Fakat bu çalışmalar ancak 2004' te bitebileceği düşünüldüğünden acil ihtiyacı karşılamak için 802.11i standartlarına uygun geçici bir güvenlik sistemi Wi-Fi tarafından oluşturulmuştur. [8]

WPA, WEP protokolünün eksiklerini gidermesi için Wi-Fi Alliance ve IEEE tarafından geçici olarak geliştirilmiş bir protokoldür. Mevcut cihazlar üzerinde yazılım güncellemesi veya değişikliği yapılarak kullanılabilen bir protokoldür. Herhangi bir donanımsal değişiklik gerektirmediğinden dolayı bu protokole geçiş hızlı bir şekilde gerçekleşmiştir. [1]

WPA'nın WEP protokolüne tercih edilmesinde üç önemli sebep bulunmaktadır. Bunlar, 802.1X/EAP tabanlı karşılıklı asıllama sağlaması ; WEP'e göre daha güçlü bir şifreleme yöntemi olan TKIP (Temporal Key Integrity Protocol)'i desteklemesi ; veri bütünlüğü için MIC (Michail- Message Integrity Check) yöntemini kullanması ve anahtar yönetim mekanizmasıdır. Bu üç madde WEP protokolünün tam olarak gerçekleştiremediği güvenirlik, erişim kontrolü ve veri bütünlüğünü gerçekleştirmek üzere WPA protokolüne yerleştirilmiştir. Buna rağmen WPA geçici bir protokoldür. Tam anlamıyla güvenlik 802.11i standardının getirdikleriyle sağlanmıştır. [8]

WPA, "hızlı paket anahtarlama" olarak bilinir ve WLAN üzerindeki her paketin üretilen tek bir anahtarla şifrelenmesi tekniğidir. Bu çözümde paketler için hızlı bir şekilde anahtar üreten kıyım (hash) tekniği kullanır. IEEE 802.11 standardı

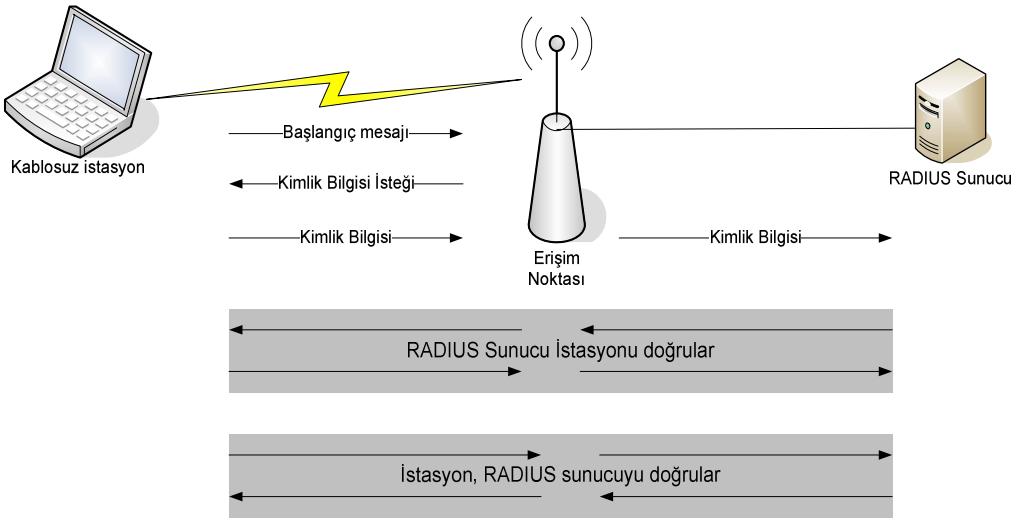
için hızlı paket şifreleme tekniğini kabul ederek, üreticilerin yeni kablosuz ürünlerde bu teknikle üretim yapmalarını sağlamıştır. [1]

4.5.1. 802.1x ile Asıllama

IEEE' nin EAP (Extensible Authentication Protocol, Genişletilebilir Kimlik Doğrulama Protokolü) standartları üzerine kurduğu bir yapıdır. WLAN veya LAN' larda kullanılmaktadır. Burada kimlik kanıtlayıcı her istemci için istemcinin tanımlayıcı bilgisine dayalı mantıksal portlar yaratmaktadır. Bu portlar denetimli ve denetimsiz portlar olmak üzere iki şekildedir. Kimlik kanıtlama öncesinde sadece denetimsiz port açıktır ve sadece kimlik doğrulama süreci için EAP trafiğine izin verilir. İstemci kimliği kanıtlandıktan sonra denetimli port açılır ve diğer yerel ağ kaynaklarına erişim hakkı verilir. [8]

802.1X asıllama süreci Şekil 4.8.'de verilmiştir. Bu süreç adımları aşağıda belirtilmiştir:

- Kullanıcı Erişim noktasına başlangıç mesajı yollar.
- Erişim Noktası kullanıcıdan kimlik bilgisi ister. Kimlik doğrulama işlemi yapılmadan EAP sürecinden başka hiç birşeye izin verilmez. Yani port kapalıdır.
- Kullanıcı kimlik bilgisini Asıllama sunucusuna (RADIUS) gönderir. Burada istemci ile asıllama sunucusu arasında EAP kaplamalı yerel ağ (EAPOL) protokolü kullanılır.
- Asıllama sunucusu asıllama işlemini gerçekleştirir.(sayısal imza ya da başka yöntemlerle yapılabilir.)
- Asıllama sunucusu kabul ya da ret cevabını erişim noktasına gönderir.



Şekil 4.8. 802.1X ile Asıllama [19]

- Erişim noktası bu cevabı kullanıcıya iletir ve kullanıcının ağa erişmesi için portlara izin verir.
- Kullanıcı asıllama sunucusundan kimliğini ister.
- Asıllayıcı sunucusu kimliğini kullanıcıya gönderir ve kullanıcı Asıllama Sunucusu asıllar ve veri trafiği başlar.

Yukarıdaki açıklamalara dikkat edildiğinde karşılıklı asıllama yapıldığı görülecektir. Eğer sistemde RADIUS sunucu yoksa paylaşılan anahtar üzerinden asıllamada desteklenmektedir.

EAP (Extensible Authentication Protocol – Genişletilebilir Kimlik Doğrulama Protokolü), noktadan noktaya iletişim için asıllama imkanı sağlayan bir protokoldür. Bu yönteme göre iletişime geçebilmek için, istemci de sunucuda dinamik olarak asıllama işlemlerini gerçekleştirmek zorundadır. Asıllama işlemini gerçekleştirebilmek için genel olarak iki yöntem kullanılması tercih edilmektedir. Bunlar parola koruması ve akıllı jetonlardır. Parola koruması, belirli bir sistemle iletişim kurmak için ilgili parolayı bilmesi prensibine dayanır. Sadece parolayı bilen

kişiler iletişime geçebilmektedir. Bu işlemleri gerçekleştirmek için, bu görev için tasarlanmış bir protokol olan PAP (Password Authentication Protocol – Şifre Kullanımlı Asıllama Protokolü) kullanılmaktadır. Parolaların RAS (Remote Access Server Uzaktan Erişim Sunucusu) sunucuya şifrelenmeden düz metin olarak gönderilmesi güvenlikle ilgili problemler yaratabilecek bir konudur. Akıllı jetonlar ise güvenli bir sunucu tarafından bir defaya özel parola üretilmesi ile gerçekleşmektedir. Bu sistemin daha profesyonel olarak ve büyük çapta çalışabilmesi için şifreleme işlemlerini gerçekleştiren RADIUS gibi özel sunucular kullanılması gerekmektedir. [15]

4.5.2. TKIP- Temporal Key Integrity Protocol (Geçici Anahtar Bütünlüğü Protokolü)

TKIP, RC4 akış şifreleyici algoritma üzerine kuruludur. TKIP, 802.11 'in güvenliğini artırıcı yani WEP'in eksiklerini tamamlayıcı yeni algoritmalar içerir. [15]

TKIP şifrelemede 48 bit başlangıç vektörü kullanılır. WEP şifrelemede 24 bitlik başlangıç vektörü, farklı veri paketlerinde sürekli kullanıldığından, IV'nin tekrarı söz konusudur. Bu durum güvenlik açısından risklidir. WPA ile birlikte gelen TKIP, 48 bitlik başlangıç vektörü kullandığından, büyük ölçüde başlangıç vektörünün tekrar kullanımı azalmış olur. [2]

TKIP, her paketin anahtarlanmasına, anahtar üretimine ve dağıtımına izin verir. WPA otomatik olarak her istasyon için tek olan anahtarları periyodik olarak üretmektedir. WPA, her 802.11 çerçevesi için tek olan anahtar kullanır. Böylece WEP'teki gibi bir anahtarın haftalarca, aylarca kullanım durumu söz konusu olmaz. [15]

TKIP, kriptografik bütünlük sağlar. WPA, veri bütünlüğü sağlamak için mesaj bütünlük kodu (MIC – Message Integrity Code) kullanır.

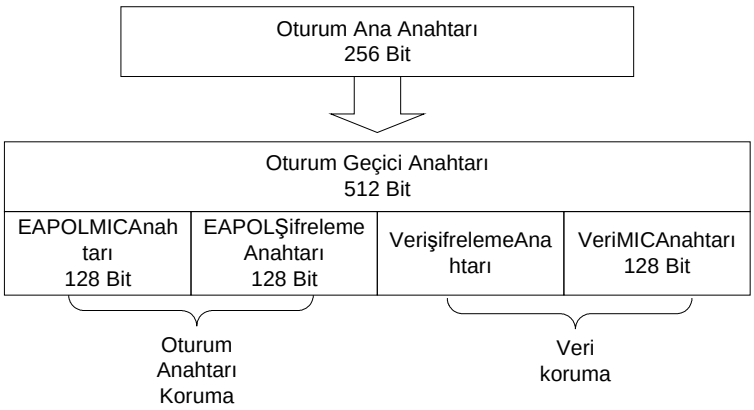
TKIP bu algoritmalarla daha önceden tartışılan pek çok saldırıya karşı koruma sağlamaktadır. WPA, WEP'in yerine standartlara dayalı olarak güvenlik

çözümleri getirmiştir. 802.11 i bu yeni algoritmalarla veri bütünlüğü ve gizliliğini sağlayacak şekilde tamamlanmıştır.[17]

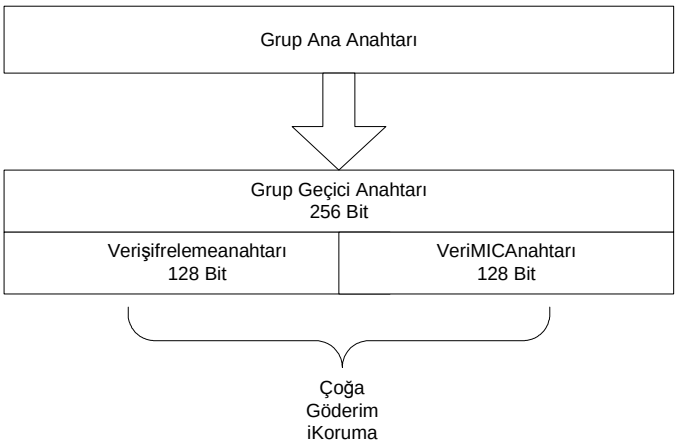
MIC (Message Integrity Code – Mesaj Bütünlük Kodu), WEP teki ICV'nin (integrity check value) zayıflıklarından dolayı, WPA ile Michael olarak bilinen bir yöntem, 8 baytlık bir mesaj bütünlüğü kodu (MIC) hesaplayan yeni bir algoritma tanımlamaktadır. MIC alanı, çerçeve verileri ve ICV ile birlikte şifrelenir. Üretilmesi ise alıcı ve gönderen MAC adresleri ve mesaj bir kıyım (hash) fonksiyonuna tabi tutulur ve 8 baytlık bir çıktı oluşur. MIC, IEEE 802.11 çerçevesinin veri bölümü ile 4 baytlık ICV arasına yerleştirilir ve daha sonra çerçeve verileri ve ICV ile birlikte şifrelenir. MIC lineer bir algoritma ile elde edilmediği için ICV gibi zayıflıkları yoktur. Bu da araya giren kişinin mesajı değiştirdiğinde anlaşılmasını sağlar. [16]

4.5.3. Anahtar Yönetimi

WEP protokolünden önemli bir fark olarak WPA'da anahtar yönetimi vardır. WPA'da 2 çeşit anahtar yapısı vardır.



Şekil 4.9. Oturum Ana Anahtarının Yapısı [19]



Şekil 4.10. Grup Ana Anahtarının Yapısı [19]

- Oturum Anahtar kümesi: 2 kablosuz cihazın haberleşmesinde kullanılır. Genelde bir kullanıcı ve erişim noktası arasında kullanılır.(Unicast haberleşmeler) Şekil 4.9.'da oturum anahtar kümesi yapısı gösterilmiştir.

- Grup Anahtar kümesi: Ağ içinde herkesin bildiği ve yayım (braoadcast) yapılması için kullanılan anahtarlar. (Multicast haberleşmeler) Şekil 4.10.'da grup ana anahtarının yapısı gösterilmiştir.

Anahtarların bir özelliği de hiyerarşik bir yapıya sahip olmalarıdır.

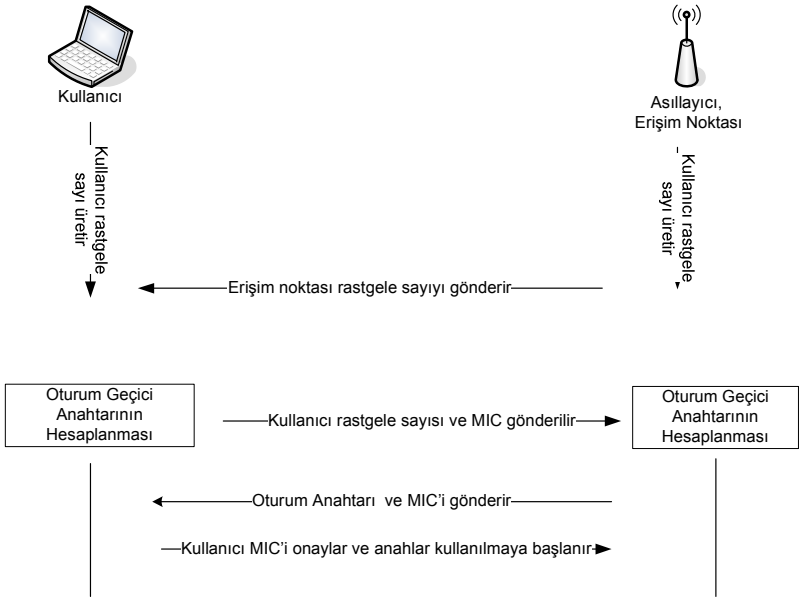
Ana anahtardan oturum ana anahtarı ve grup ana anahtarı elde edilir. Ana anahtar asıllama sırasında asıllama sunucusu tarafından üretilmiştir. Oturum ana anahtarı ile elde edilen anahtarlar geçicidir. Her yeni cihazla bağlantı yeniden kurulduğunda ya da ağdan çıkılıp girildiğinde yeniden oluşturulur. Grup Ana Anahtarları da grup geçici anahtarı ile erişim noktaları tarafından belirlenip kullanıcılara dağıtılmaktadır. [19]

Oturum Anahtar Kümesinin Üretilmesi : Bu anahtar kümesinin eldesi erişim noktası ve kullanıcı arasında belirlenir. Belirlenme biçimi Şekil 4.11' de gösterilmiş ve aşağıda açıklanmıştır.

- Erişim noktası rasgele sayı üretir ve kullanıcıya yollar.

- Kullanıcı rasgele bir sayı belirler ve geçici anahtarları elde edip, rasgele sayıyı erişim noktasına yollar. MIC oturum ana anahtarını bildiğinin kanıtıdır. Erişim noktası geçici anahtarları hesaplar.
- Buradan gerekirse grup anahtarlarını da hesaplayıp kullanıcıya gönderir.
- Kullanıcı MIC' i onayladıktan sonra anahtarları kullanmaya başlar ve bunu 4. mesaj ile bildirir.
- Erişim noktası da bu mesajı aldıktan sonra anahtarları kullanmaya başlar.

Grup Anahtar Kümelerinin Üretilmesi : Tüm ağ haberleşileceği için farklı olan oturum anahtarları kullanılamaz. Dolayısıyla herkesin paylaştığı bir anahtar olmalıdır ve buda grup anahtarlarıdır. Grup anahtar kümesinin eldesi şekil 4.12'de gösterilmiş ve aşağıda açıklanmıştır.



Şekil 4.11. Oturum Anahtarının Üretilmesi [19]

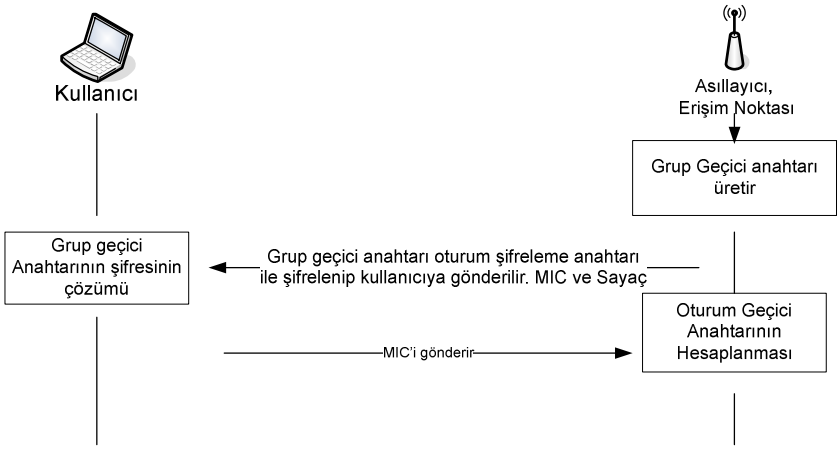
- Oturum anahtarları kümesi hesaplandıktan sonra, erişim noktası Grup geçici anahtarını kendi oluşturur.

- Bir önceki aşamada elde edilmiş olan oturum şifreleme anahtarı ile şifreleyip kullanıcıya gönderir. MIC burada mesaj bütünlüğünü sağlar. Sayaç ise tekrar saldırılarını önlemek içindir.

- Kullanıcı Grup geçici anahtarını şifreyi çözerek elde eder ve kullanmaya başlar.

Erişim noktası sayacı bir artırarak MIC (mesajın geçerli olduğunu belirtmek için) ile birlikte gönderir, erişim noktası da grup geçici anahtarını kullanmaya başlar.

Farklı Anahtar Üretimi :WEP şifrelemede aynı anahtar ile şifrelenmiş çerçevelere dayalı saldırılar yapılabilmekteydi. WPA' da bu saldırıları engellemek için her paket için farklı anahtarlar üretilmesi öngörülmüştür. Yeni anahtar hesaplamaları iki aşamada gerçeklenir. iki aşama olmasının nedeni WEP tabanlı cihazların yüksek işlem yapabilme kapasitenden yoksun olması ve işlem sayısını en aza indirgenmek istenmesidir.



Şekil 4.12. Grup Anahtarı Kümesi Eldesi [19]

4.6. WPA2 (Robust Security Network, IEEE 802.11i)

WPA, WEP tabanlı bir yapı olduğu ve eksiklerinin çıkabileceği şüphesinden dolayı (RC4 algoritmasının zayıflıkları) IEEE 802.11 i standartlarına uygun yeni bir protokol geliştirilmiştir. Bu protokol WEP üzerine kurulmamış yeni ve farklı bir yapı olarak geliştirilmiştir. Standartlaşması 2004 yılında tamamlanmıştır. RSN (Çok Güvenli Ağ) WPA' yı desteklemekte fakat WEP'i desteklememektedir. Çünkü WEP, artık bir güvenlik unsuru olarak görülmemektedir. [2]

RSN asıllamayı ve anahtar yönetimini IEEE 802.1X standartları ile gerçekler. Veri bütünlüğü MIC ile sağlanır. Bu yapı gezginlik (roaming) hareketlilik sağlar. Gezginlik gerçek zamanlı iletişimlerde önem kazanır çünkü veri kaybını engeller. RSN gezginliği iki farklı şekilde gerçekler. [18]

- Önceden asıllama: Önceden 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 erişim noktasına 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.

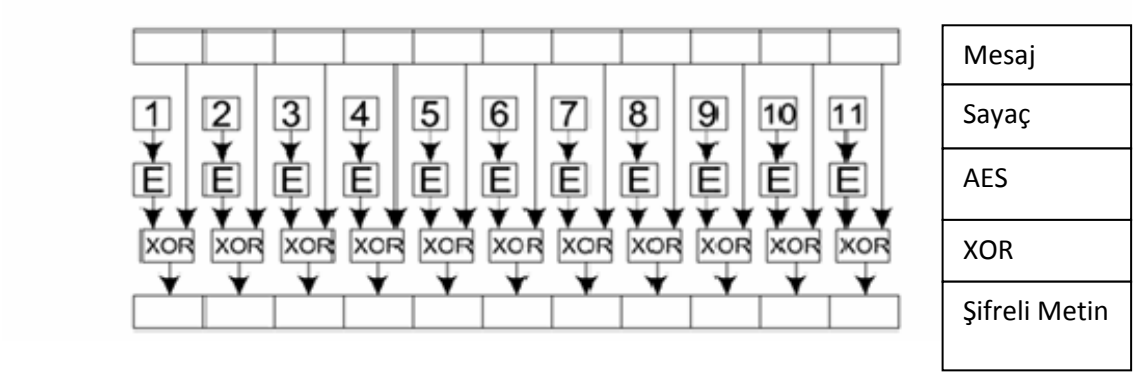
RSN' de şifreleme Temporal Key Integrity Protocol (TKIP) veya Counter Mode with CBC-MAC Protocol (CCMP) ile gerçeklenir. CCMP zorunlu iken, TKIP ise seçeneklidir. [18]

4.6.1. 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 bir çok kullanım modu vardır. [2] 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 4.13'te sayaç yöntemi gösterilmiştir. [19]

Şekil 4.13'te de görüldüğü gibi veri blokları şifrelenmiş sayılar ile dar veya işlemine tutulmaktadır. Burada kullanılan sayılar rasgele seçilmektedir çünkü aynı iki mesaj aynı çıkışları verecektir. Bu sayının başlangıcı karşı tarafa iletilmelidir. Bu modda 128 bitlik şifreleme anahtarı kullanılır.[19]



Şekil 4.13. AES (sayaç) çalışma modu [19]

- CBC- MAC (Cipher Block Chaninig Message Authentication Code) modu (Bütünlük) : CBC-MAC modu ise MIC hesabında kullanılır. Eğer mesajda 1 bit değişirse MIC de büyük değişiklikler olur ve tahmin edilemez. MIC' in hesaplanmasında ilk veri bloğu alınır ve AES şifreleme kullanarak şifrelenir. Sonuç ile 2. veri bloğu dar veya işlemine tutulur ve şifrelenir. Çıkan sonuç bir sonraki blok ile dar ve ya işlemine tutulur ve şifrelenir. MIC hesabı geri dönülmez bir şekilde yapıldığı için araya girenin mesaja uygun bir MIC hesaplaması mümkün değildir. [18]

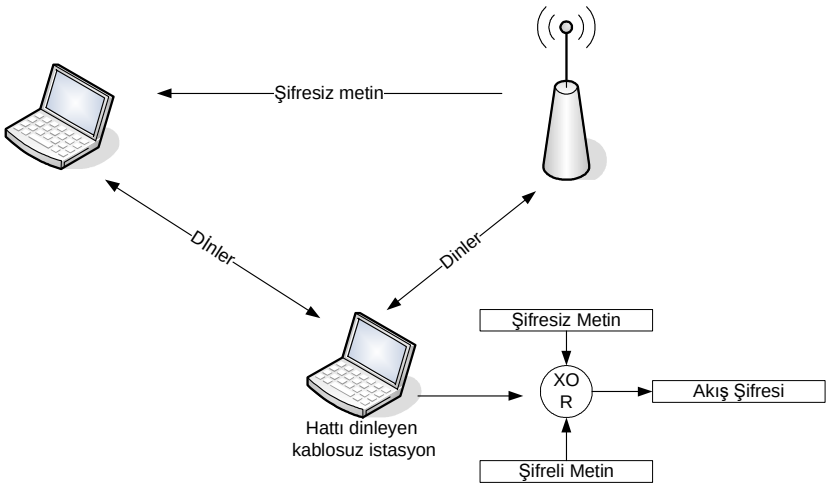
4.7. 802.11 Standardının Güvenlik Açıkları

Daha öncede belirtildiği gibi, 802.11 tabanlı WLAN'larda güvenlik için WEP protokulü kullanılır. WEP protokolü, trafiği korumak için değişik anahtar uzunluğuna sahip RC4 kriptografik algoritmasını kullanır. Tekrar belirtmek gerekirse, 802.11 standardı 40 bitlik WEP kriptografik anahtarı kullanır. Fakat bazı üreticiler ürünlerinde, 104 bitlik hatta 128 bitlik anahtarları entegre ederek sunmaktadır. RC4 algoritmasında kullanılan gerçek anahtar, 128 bitlik WEP anahtarına, 24 bitlik başlangıç vektörünün de (IV) eklenmesi ile, 152 bit olur.

Güvenlik ile uğraşanlar, 802.11 standardında güvenlik problemleri olduğunu ortaya koymaktadır. Bunlar pasif ataklar olabildiği gibi, aktif ataklar da olabilmektedir.

WEP Protokolünün Güvenlik Problemleri:

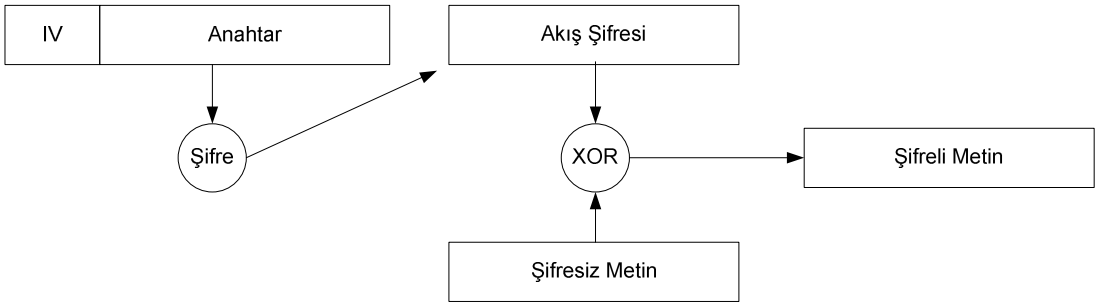
Statik WEP anahtarlarının kullanımı, en çok bilinen güvenlik açığıdır. Kablosuz ağlarda birçok kullanıcı benzer anahtarları uzun zaman periyodlarında kullanmaktadır. Bu WEP protokolünde herhangi bir anahtar yönetimi kullanılmamasından kaynaklanmaktadır. Bir mobil cihaz örneğin bir dizüstü bilgisayar kaybolduğunda yada çalındığında, bu anahtarı paylaşan diğer bilgisayarlar da tehlikeye atılmış olur.



Şekil 4.14. Ortak Anahtar Kimlik Asıllama yönteminin zayıflığı [23]

Eğer istasyonlar aynı anahtarı kullanırsa, hattı dinleyenlerin oluşturduğu çok büyük bir trafik oluşur. Şekil 4.14' te de hattı dinleyen bir istasyonun akış şifresini kolay bir şekilde ulaşabildiği görülmektedir. [23]

Şekil 4.15.'te gösterildiği gibi, WEP içerisinde kullanılan başlangıç vektörü IV, gönderilen mesaj içerisinde 24 bitlik bir bölümdür. RC4 algoritması tarafından üretilen akış şifresinin (key stream) oluşumu sırasında kullanılan bu 24 bit, kriptolojik amaçlar için kullanıldığında çok küçük bir alandır. Aynı başlangıç vektörünün tekrar tekrar kullanımı, veriyi korumak için kullanılan bu akış şifresinin aynı olmasına neden olmaktadır ve trafiği yoğun ağlarda bu anahtar sürekli olarak tekrar etmektedir. Bunun yanı sıra 802.11 standardında başlangıç vektörlerinin nasıl ayarlanacağı ve değiştirileceği ile ilgili tanımlamalar bulunmamaktadır. Ayrıca genellikle aynı firmanın kablosuz ağ arabirim kartlarına bakıldığında genellikle aynı başlangıç vektörü dizisi ürettikleri veya bazı kablosuz ağ arabirim kartlarının aynı başlangıç vektörünü kullanabildikleri görülmektedir. Sonuç olarak, şifre çözücü kötü niyetli kişiler, ağ trafiğini kaydederek, akış şifresini bulabilirler ve şifreli metnin (cipher-text) şifresini çözebilirler. [23]



Şekil 4.15. Başlangıç Vektörü IV ile Şifreleme [23]

WEP içinde kullanılan başlangıç vektörü IV, RC4 şifreli anahtarın bir parçasıdır. Hattı dinleyenler, her pakette RC4 algoritmasının zayıf anahtarı ile 24 bitlik bir bilginin birleştiğini bilir ve ağ trafiğinin çok küçük bir bölümünü ele geçirip, analiz ederek anahtarı ele geçirebilir. Şekil 4.15' te başlangıç vektörü ile şifreleme gösterilmiştir.

WEP herhangi bir kriptolojik bütünlük koruması sağlamaz. Bununla birlikte 802.11 MAC protokolü paketlerin bütünlüğünü kontrol etmek için kriptografik olmayan Dönüşsel Yedeklilik Kontrolü (CRC) kullanır ve paketlerin alınıp alınmadığına ait özet tutar. Kriptografik olmayan bu özetler çok tehlikelidir ve saldırılara davetiye çıkarır. Bu saldırılar, saldırganların herhangi bir mesajın şifresini çözmesine, mesajın ve erişim noktasına gönderilen CRC'nin ve paketin gönderilip gönderilmediği bilgisinin değiştirilmesine izin veren aktif saldırılardır. Aktif saldırılar, paketlerin deşifre ederek, içerisini değiştirebilirler. Bu tip saldırılar, çoğu zaman güç farkedilirler ve kriptolojik bütünlük koruması içermeyen (noncryptographic integrity protection) bu şifreleme protokollerinde, şifrelenmiş metni ele veren diğer protokollerle etkileşim olasılığından dolayı riskleri göz önüne alarak planlama yapmak gerekir. [23]

WEP ve 802.11 WLAN güvenliği ile ilgili problemler aşağıda verilmiştir.

- Ürünlerde güvenlik özelliklerinin aktif olmaması

Kullanıcıların ürünleri alıp, kurduklarında güvenlik özelliklerini aktif hale getirmeleri gerekir. Her ne kadar yetersiz de olsa en kötü güvenliğin hiç olmamasından daha iyi olduğu göz önüne alınmalıdır.

- Başlangıç vektörünün çok kısa yada statik olması

24 bitlik başlangıç vektörü üretilen akış şifresinin sürekli tekrarına sebep olmaktadır. Tekrarlar, verinin kolay bir şekilde deşifre olmasına sebep olmaktadır.

- Kriptografik anahtarların kısa olması

Kullanılan 40 bitlik anahtarlar hiçbir sistem için yeterli değildir. Genellikle anahtar uzunluğunun 80 bitin üzerinde olması istenir. Uzun anahtar, saldırılara daha az maruz kalma anlamına gelir.

- Kriptografik anahtarların paylaşılması

Kriptografinin temeli, sistemin güvenliğinin büyük oranda anahtarların gizliliğine bağlı olmasıdır. Paylaşılan anahtarlar sistemi tehlikeye atmaktadır. Anahtarı paylaşan kişi sayısının artması güvenlik riskini de arttırmaktadır.

- Kriptografik anahtarların otomatik olarak yada belli zaman aralıklarında güncellenmemesi

Kriptografik anahtarların, saldırıları önleme adına sık sık değiştirilmelidir.

- RC4'ün yetersiz anahtarı ve WEP içinde uygun şekilde kullanılmaması

24 bitlik başlangıç vektörünün kolay bir şekilde açığa çıkabilmesi ile RC4 akış şifresindeki yetersizliğin birleşmesi sonucu, yapılan saldırılarda anahtarlar ele geçirilebilmektedir. RC4'ün diğer birçok uygulamasında herhangi bir zayıflık yetersizlik yoktur. Çünkü anahtar bitleri açığa çıkmaz ve her pakette anahtar programı yeniden başlatılmaz.

- Paketin bütünlüğünün sağlanaması

CRC32 ve diğer lineer blok kodları, kriptolojik bütünlük sağlama konusunda yetersizlerdir. Mesajın değişmesi olası bir durumdur. Lineer kodlar, saldırılara karşı veri bütünlülüğünü sağlama konusunda yetersizdir. Saldırılara karşı kriptografik koruma gereklidir. Kriptografik olmayan protokoller saldırıları kolaylaştırmaktadır. [20]

- Kullanıcıların kimliklerinin doğrulanmaması

Sadece cihazların kimlikleri doğrulanmaktadır. Cihazların herhangi bir şekilde kaybolması yada çalınması durumunda ağa ulaşması mümkündür.

- Kimlik doğrulaması aktif olmaması sadece basit bir ağ kimliği (SSID -Service Set IDentifier) doğrulaması yapılması

SSID ağ yöneticisi tarafından ayarlanan gizli bir anahtardır. 802.11 ağına bağlanmak isteyen bir kullanıcı SSID numarasını bilmek durumundadır. Ancak kablosuz ağ çözümleyicileri bile SSID numarasını yakalayabilmektedir. Çünkü başlangıçta SSID, WLAN üzerinden gönderilen her paketin başlığının bir parçasıdır.

Kablosuz ağlarda, kimlik-tabanlı sistemler (identity-based system) saldırılara oldukça açıktır. Çünkü çok kolay bir şekilde araya girilerek hat dinlenebilmektedir. [8]

- Aygıt kimlik doğrulamasının, basit bir paylaşılmış anahtar ile istek cevap şeklinde olması

Tek yönlü istek cevap kimlik doğrulaması hattın habersiz dinlenip gidip gelen mesajların içeriğinin değişmesini sağlayabilen ortadaki adam saldırılarına davetiye çıkarır. Iki yönlü yani karşılıklı kimlik doğrulama (mutual authenticatin-bidirectional authentication) yöntemi, kullanıcıların ve ağın gerçek olduğunun doğrulanması için gereklidir. [20]

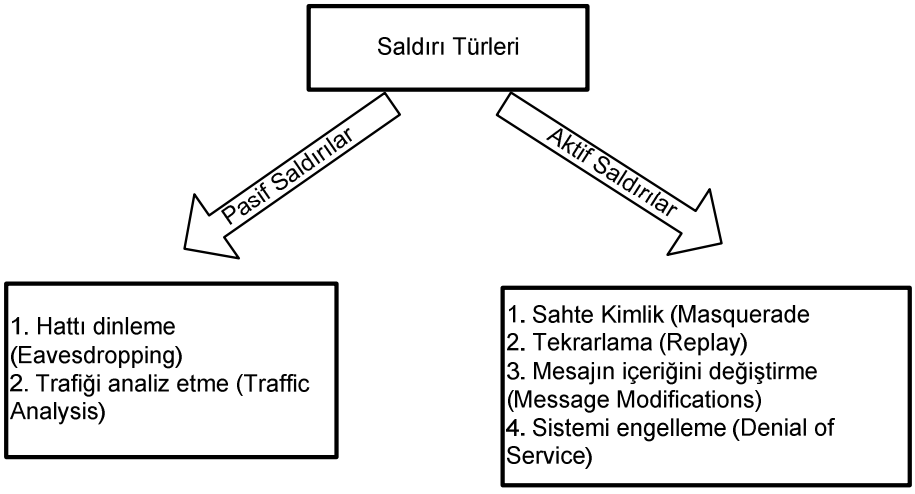
- İstasyonun kimliğinin erişim noktası tarafından doğrulanmaması

Erişim noktasına izinsiz kullanıcıların erişiminin engellenmesi için istasyonların erşim noktası tarafından doğrulanması gerekir.

4.8. Güvenlik İsterleri ve Tehditler

802.11 WLAN endüstrisi, son yıllarda gelişmeye başlamış ve gelişimi hız kazanmıştır. Tüm göstergeler teknolojinin kablosuz yönde gittiğini göstermektedir. Önümüzdeki birkaç yıl içerisinde bir çok organizasyon 802.11 WLAN teknolojisini kullanmayı planları arasına alacaktır. Günümüzde de yavaş yavaş, havaalanı, alışveriş merkezi ve hastane gibi halka açık noktalarda bu teknolojiyle hizmet verilmeye başlandığı görülmektedir. Bu teknoloji her ne kadar da büyük bir hızla gelişmekte ve uygulanmaya başlanmakta olsa da yayınlanan raporlar 802.11 ağların çok fazla miktarlarda saldırılara maruz kaldığını ve güvenlik risklerinin bulunduğunu ortaya koymaktadır. [8]

Şekil 4.16'da güvenlik saldırıları bir şema ile gösterilmiştir. Yukarıda bahsedildiği gibi, yapılan saldırılar pasif ve aktif olmak iki bölüme ayrılmıştır. Bu iki saldırı türüde kendi arasında çeşitli alt türlere ayrılmaktadır.



Şekil 4.16. Genel Saldırı Türleri

Pasif Saldırılar: Bu tip saldırıların özelliği, ağdaki herşeye ulaşabilmek ancak içeriğini değiştirememektir. Yani hattı dinleyebilmekte ancak içeriğine dokunamaktadırlar. Bu saldırılar, ağ trafiğini analiz etme yada hattı dinleme şeklinde olabilmektedir. [8]

Hattı dinleme (Eavesdropping) : Bu tip saldırılarda mesajın içi görüntülenir, izlenir.

Ağ trafiğinin analizi (Traffic Analysis): Bu tip saldırılarda iletişim kuran taraflar arasında giden gelen mesajların büyük bir bölümü kontrol altında tutulur.

Aktif Saldırılar: Bu saldırılar mesajların, dosyaların içeriğini değiştirebilir. Bu tip saldırıları yakalamak olasıdır ancak önlemek mümkün değildir. Aktif saldırılar dört ayrı altbaşlıkta incelenebilir. [8]

Sahte Kimlik (Masquerading): Bu tip saldırılarda, saldırgan giriş ağa giriş yetkisi olan bir kullanıcı gibi ağa girer ve onun haklarını kullanabilir.

Tekrarlama (Replay): Saldırgan pasif ataklarda olduğu gibi iletimi izler ve yasal bir kullanıcı gibi mesajı tekrar iletir.

Mesajın İçeriğini Değiştirme (Message Modification): Saldırgan mesajın içeriğini değiştirebilir, silebilir. [8]

Hizmeti engelleme (Denial of service): Bu saldırı türü normal ağ kullanımı veya iletişimi engeller.

4.8.1. Gizliliğin Azalması

Gizlilik, kimliği doğrulanmamış kişilerin, bilgilere ulaşamamasıdır. Bu en temel güvenlik isteğidir. Kablosuz teknolojinin radyo dalgalarını kullanarak yayılım yapmasından dolayı gizlilik konusu kablosuz ağlarda karşılanması zor bir güvenlik

isteridir. Ağ kaynaklarına ulaşmak için herhangi bir kablo bağlantısına gerek bulunmadığından güvenliği sağlamak daha zordur. Ayrıca, iletişimin meydana geldiği mesafeyi kontrol altına almak imkansız olabildiğinden kablolu ağlarda kullanılan güvenlik tedbirleri kablosuz ağlarda etkili olamamaktadır.

Sadece 802.11 kablosuz ağ kullanılan ortamlarda, pasif dinleme (passive eavesdropping) büyük bir risk faktörüdür. Bu tip saldırılar sırasında, saldırgan iletişimin dinleyebildiği gibi, özel bilgiler, ağ tanımlayıcısı, şifreler veri konfigürasyonu gibi kritik bilgileri de ele geçirilebilmektedir. 802.11 sinyalleri binalar arasında da yayılabildiğinden kapsama alanı genişledikçe binanın parkından yada yoldan bile kablosuz ağın algılanması ve dolayısıyla saldırı mümkündür. Kablosuz ağ çözümleyici araçları da (sniffer) bu tip pasif saldırıları kullanır. Bu tip saldırılarla, iki sebepten dolayı çok karşılaşılır. Bunlardan birincisi WLAN teknolojisinin gizlilik özelliğinin aktif edilmemesinden, ikincisi ise 802.11 ağlarda yukarıda da belirtildiği gibi saldırıya açık çok fazla alan bulunduğundandır.[20]

Günümüzde, kablosuz paket çözümleyici araçlarına, internet üzerinden kolayca ulaşılabilir. Bu araçlar ağ analizi yapmak için kullanılbildiği gibi ağı kırmak için yani izinsiz girmek için de kullanılabilir. Bu yazılımlardan bazıları, RC4 şifrelemenin kullandığı algoritmanın kusurlarını örtecek avantajlar sağlar. Bunu gerçekleştirmek için ise Linux işletim sistemi kurulu bir bilgisayar ve kablosuz ağ kartı yeterlidir. Bu yazılım pasif olarak WLAN veri iletimini izler ve izlediği 100Mb'lık paketle şifrelenmiş anahtarları ele geçirir. Ağ trafiğinin yoğun olduğu yerlerde bu miktarda veriyi toplamak üç dört saat alır. Yoğunluk yaşanmayan yerlerde ise bir iki gün sürebilir. En az 100 MB'lık verinin toplanmasından sonra, aynı akış şifresini kullanan iki şifreli metin (cipher text) ele geçirilmiş olur ve veri bütünlüğü ve gizliliği tehlikeye girmiş olur. Böylelikle kötü niyetli kullanıcılar, WEP anahtarını ele geçirmiş olur ve WLAN üzerinden gelen giden tüm paketleri okuyabilir. [20]

Veri kaybının konusundaki diğer bir risk ise, erişim noktasının anahtar (Switch) yerine göbeğe (hub) bağlandığında, herhangi bir gelişi güzel dizüstü

bilgisayardan ağ trafiğinin izlenebilmesi olasılığıdır. Çünkü göbekler, genellikle tüm ağ trafiğini, bağlı tüm cihazlara yayımlarlar. Buna karşı anahtarlar, belirli cihazlar dışındaki girişleri yasaklayarak araya izinsiz girerek hatta dinlemeye karşı ağı korumuş olurlar. Yani kablosuz bir erişim noktası bir ethernet göbeğine bağlandığında, trafiği izleyen bir kablosuz cihaz, kablolu yada kablosuz istasyonların verilerini alabilir. Sonuç olarak, erişim noktalarının bağlantılarında göbek yerine anahtar kullanımı daha doğru bir çözüm olarak görülmektedir.

Veri gizliliğinin sağlanamaması konusundaki diğer bir riskte aktif saldırılardır. İzleyici yazılımlar (sniffing software) kullanıcı isimlerini ve şifreleri hatta ağ üzerinden gelen giden verileri yakalayabilir. Dolayısıyla ağa girmeye çalışan birisi yasal bir kullanıcı gibi ağa bağlanarak, erişim noktası üzerinden kablolu ağa ulaşabilir ve bazı araçları kullanmak suretiyle ağı tarayabilir. Ağı dinleyen bu kişiler isterlerse kullanıcı isimlerini, şifreleri ve IP adresleri gibi bilgileri kullanarak ağ kaynaklarına ve kritik şirket verilerine ulaşabilir.

Diğer bir risk ise sahte erişim noktalarıdır. Örneğin gizlice ofis içersinde bir yere mesela bir masanın altına yerleştirilen erişim noktası büyük bir risk oluşturmaktadır. Bu erişim noktaları yetkisiz kişilerin ağ kaynaklarına erişmesine izin vermek için kullanılır. Bu erişim noktası, WLAN kullanıcılarına yakın olduğunda, istasyonlar tarafından ağdaki gerçek bir erişim noktası gibi görünecek şekilde konfigure edilir ve böylece bu erişim noktası kendisinin ağdaki geçerli bir erişim noktasını olduğuna istasyonları inandırır. Sonuçta istasyonların gönderdiği veriler bu erişim noktası üzerinden gönderilecektir. Bu sahte erişim noktası, gerçek erişim noktaları ile istasyonlar arasında geçen kablosuz trafiği yakalayabilmektedir. İstasyon trafiğini yakalamak için sahte erişim noktalarının tek ihtiyacı gerçek erişim noktalarında daha güçlü bir sinyaldir. Tüm bunların yanısıra, kötü niyetli kullanıcılar, kimlik doğrulanmadan erişime izin verecek şekilde konfigure edilmiş gerçek erişim noktalarını kullanarak da kaynaklara ulaşabilirler. Diğer önemli bir nokta, sahte erişim noktalar sadece kötü niyetli kullanıcılar tarafından kullanılmayacağıdır. IT bölümünün haberi olmadan, kablosuz teknolojinin avantajlarından yararlanmak

isteyen kullanıcılar sahte erişim noktalarını kullanabilmektedir. Ek olarak, güvenlik ve ağ yöneticisinin haberi olmadan kurulan bu erişim noktaları çoğu kez, güvenlik konfigürasyonları yapılmadan kurulmaktadır. [23]

4.8.2. Veri Kaybı

Kablosuz ağlardaki veri bütünlüğü, kablolu ağlardakine benzerdir. Bunun sebebi organizayonların gerek kablolu gerekse kablosuz ağ uygulamalarında verinin korunmasını sağlayacak yeterli kriptografik yöntem kullanmamalarıdır. Dolayısıyla veri bütünlüğünün sağlanması zor bir hale gelmektedir. Örneğin, kablosuz sistem üzerindeki bir kullanıcının gönderdiği e-posta içindeki verinin silinmesi yada değiştirilmesi verinin bütünlüğünü tehlikeye atar. Çünkü 802.11 standardı içerisinde bulunan güvenlik özellikleri veri bütünlüğünü sağlama konusunda yetersizdir. Ayrıca aktif saldırılar dolayısıyla, sadece veri bütünlüğünün değil sistem bütünlüğünün de tehlikeye girmesi olasıdır. Kriptografik Kontrol mekanizmaları (örneğin mesaj doğrulama kodları ve hash gibi) kullanılmadığında, mesajların içeriğinin değiştirilmesini sağlayacak saldırılara maruz kalınması olasıdır.

4.8.3. Ağın Servis Dışı Kalması

Ağın işlerliğini tehlikeye atan örneğin, güvenlik sisteminin normal işlemesini durdurmak için sinyaller gönderen saldırılarda (jamming) vardır. Bu durdurma saldırıları, kötü niyetli kullanıcıların ağın kablosuz sinyalini bozmak için bir kablosuz aygıttan kasten yaydıkları sinyallerle gerçekleşir. Ayrıca kablosuz telefonlar ve mikrodalga fırın yayılımları da bu duruma istemeden de olsa sebep olmaktadır. Durdurma (Jamming) sinyalleri ilerişimin bozulmasına sebep olurlar. Çünkü ağın gerçek kablosuz sinyali işlevini yerine getiremez duruma gelir. [14] Bunun yanısıra kötü niyetli ve kasıtlı olmadan bazı kullanıcılar sistemin servis dışı kalmasına (DOS-Denial of Services) sebep olmaktadır. Örneğin, çok yüksek boyutlarda dosya indiren bir kullanıcı istemeden de olsa kablosuz sinyali tek eline almış ve böylece diğer kullanıcıların ağı kullanmasını engellemiş olur. Sonuçta bunun önüne kullanıcıların kablosuz ağ üzerinden indirebilecekleri veri miktarının ve tipinin sınırlandırılması yoluyla çözüm bulunabilir. [2]

4.8.4. Diğer Güvenlik Riskleri

Kablosuz aygıtların yaygınlaşması ile, birçok kullanıcı, kendi şirketlerine uzaktan bağlanabilmek için çeşitli yollar aramaktadır. Örneğin bunlardan biri, güvensiz, üçüncü tür ağlar (untrusted third party) kullanmaktır. Birçok şirketin konferans salonlarında, konferans anında internete yada şirketin ağına bağlanmayı sağlayacak kablosuz ağ bulunmaktadır. Havaalanları, oteller, bazı kafeteryalar müşterilerine herkesin ulaşabileceği 802.11 tabanlı kablosuz ağ hizmeti vermeye hatta VPN ile bağlantı sunmaya başlamışlardır. [20]

Bu tür güvensiz (untrusted third party) ağlar üç ana risk faktörünü de beraberinde getirmektedirler.

Bu ağlar herkesin kullanımına açık olduğu için kötü niyetli kullanıcılar da kullanabilmektedir.

Bu ağlar kullanıcının kendi ağındaki bir köprü gibi davranırlar. Böylece herkese açık ağ üzerinden şirket ağına saldırı ve kaynaklara erişim olası hale gelir.

Yüksek kazançlı antenlerin kullanımı kapsama alanını artırdığından kötü niyetli kullanıcıların kablosuz sinyali çok kolay bir şekilde dinleyebilmelerine neden olur.

Her ne kadar organizasyonlar kendi kullanıcıları ve ağları için önlemler almaya çalışsa da, kullanıcıların kendi ağlarına güvensiz ağ üzerinden bağlanmaları organizasyon için saldırıya açık noktalar yaratabilmektedir. Kullanıcılar, ağ kaynaklarına ister özel ister herkese açık bir yöntemle olsun ulaşmak isterler. WLAN kullanıma açılacaksa, uygulama katmanı protokolü (Application Layer Protocol) örneğin Taşıma Katman Güvenliği (Transport Layer Security) yada Güvenli Soket Katmanı (Secure Socket Layer –SSL) kullanarak kaynakları korunmasını sağlanabilir. Ancak pek çok ofiste bu tip yöntemleri kullanmaya gerek görmemektedir. Çünkü bilgilern herkese açık olmasının bir sakıncası yoktur. Özel kaynaklar için güvenliği sağlamak konusunda da VPN bağlantı kullanılabilir. Çünkü

bu yöntem hattın dinlenmesini ve yetkisiz kişilerin özel kaynaklara erişimini engellemektedir.

Sonuç olarak, kablosuz ağ kurma aşamasında tüm bu güvenlik konularını dikkate almak gerekmektedir.

5. RİSKLERİ AZALTMA YÖNTEMLERİ

Ülkeler devletle ilgili birimlerde, adrese yönelik tehditlere ve saldırıya açık noktalara karşı önlemler alarak riskleri azaltmaya çalışmaktadırlar. Yönetimsel önlemleri, operasyonel ve teknik önlemlerle birlikte kullanıldığında WLAN sistemlere yönelik riskleri azaltma konusunda daha etkili olmaktadır. Aşağıdaki hususlar tüm saldırılara karşı önlem olmasa da bu önlemler güvenli kablosuz ortam için gereklidir.

5.1. Yönetimsel Önlemler:

Güvenli kablosuz ağlar için alınacak yönetimsel önlemler kapsamlı bir güvenlik politikası ile başlar. Güvenlik politikası ve bu politikaya riayet etme, alınacak diğer operasyonel ve teknik önlemler için temel teşkil eder. WLAN ortamı için tanımlanacak kurallar, aşağıdaki hususları karşılamalıdır.

Kimlerin kablosuz teknolojiyi kullanacakları tanımlanmalıdır.

Internet bağlantısının gerekli olup olmadığı belirlenmelidir.

Kimlerin erişim noktası ve diğer kablosuz aygıtları kurup kuramayacağı belirlenmelidir.

Kablosuz bağlantı üzerinden gönderilecek verilerin tipi belirlenmelidir.

Hangi tip kablosuz aygıtlara izin verileceği belirtilmelidir.

Erişim noktaları için güvenlik ayarlarının tanımlanması gerekir.

Hangi alanda hangi kablosuz cihazın kullanılabileceği ile ilgili sınırlamalar tanımlanmadır.

Tüm kablosuz cihazların yazılım ve donanım konfigürasyonu tanımlanmalıdır.

Güvenlik ile ilgili ve kablosuz aygıtlarla ilgili kayıpları raporlayan bir yönlendirici kılavuz tedarik edilmelidir.

Bilgi hırsızlığını azaltmak için kablosuz kullanıcıların korunmasını sağlayacak yönlendirici kılavuz oluşturulmalıdır.

Şifreleme ve anahtar yönetimi kullanımı için yönlendirici kılavuz oluşturulmalıdır.

Bunların yanısıra, kablosuz teknolojiyi kullanacak personele eğitim verilmesi gerekmektedir.

Ayrıca ağ yöneticilerinin WLAN sistemlerinin ve cihazlarının karşı karşıya kaldığı güvenlik risklerinden haberdar olmaları gerekmektedir. Ağ yöneticileri, güvenlik politikasına uyulmasını sağlamalı ve herhangi bir saldırı anında hangi aksiyonların alınacağını bilmelidir.

Sonuç olarak; güvenlik için en önemli önlem eğitilmiş ve bilinçli kablousz ağ kullanıcılardır.

5.2. Operasyonel Önlemler

Sadece yetkili kullanıcıların kablosuz ağ ekipmanlarına erişiminin sağlandığından emin olmanın en temel adımı fiziksel güvenliktir. Fiziksel güvenlik, erişim kontrolleri, personel tanımlamaları, dış sınır korumaları gibi ölçütlerle birleştirilmelidir. Aynı kablolu ağlarda olduğu gibi, kablosuz ağ tarafından kullanılan servislerde, fiziksel erişim denetleyicilerine ihtiyaç duyarlar. Örneğin fotoğraf tanıma, kimlik kartı okuyucu yada biyometrik cihazlar (kimlik tanıma için parmakizi, retina gibi kişiye özgü öznitelikler kullanan cihazlar) kablosuz sistemlerde kullanıldığında, uygunsuz giriş risklerini en aza indirmektedir. Fiziksel erişim denetimi için kullanılan biyometrik sistemler, retina tarayıcılar, iris tarayacılar, parmakizi, yüz ve ses tanıyıcılar gibi aygıtları içerir. Dış sınır koruma olarak

yukarıda bahsedilen fiziksel güvenlik önlemlerine kapıların kilitlenmesi, erişim noktaları gibi kablosuz ağ birimlerine izinsiz girişleri bir miktarda olsa önlemek için çeşitli yerlere video kamera kurulması diğer koruma önlemleri olarak söylenebilir.

Diğer önemli bir noktada WLAN alanı içersinde erişim noktalarının nerelere yerleştireleceğine karar vermektir. Erişim noktalarının kapsama alanı, bina duvarlarını aştığında, güvenlikle ilgili açıklar meydana gelecektir. Örneğin binanın dış alanında kablosuz cihaz kullanılarak ağ trafiği izlenebilir. Bir binadan diğerine köprü ile bağlantı kurulduğunda da aynı durum söz konusudur. En ideali, erişim noktalarının stratejik olarak bina içerisine yerleştirilmesidir, böylece kapsama alanı binanın dışına taşmamış olur. Organizasyonlar, erişim noktalarının alanını ölçmek için kablosuz ağın kurulduğu binanın içinde ve dışında site alanını ölçme araçları (site survey tools) kullanmalıdırlar. Bunun yanısıra, organizasyonlar kablosuz güvenlik değerlendirme araçları ve programlı ve muntazam bir şekilde güvenlik denetlemeleri yapmalıdırlar.

Site alanını ölçme araçları, erişim noktalarının kapsama alanını ölçmektedir. Bazı üreticiler site alanı ölçme araçlarına, erişim noktasından çıkan sinyalin gücünü ölçen özellikleri de koymuşlardır. Bu ölçümler kapsama alanının ayrıntılı olarak planlanmasında kullanılır. Bazı erişim noktası üreticileri, erişim noktalarının güç seviyesinin kontrolüne izin veren özellikler eklemişlerdir. Bu özellik kapsama alanının çok geniş olmaması istenen yerlerde kullanışlıdır. Örneğin bir bina yada odada kablosuz bağlantı gerekiyorsa, kapsama alanının küçük olması gerekir. Bu şekildeki küçük alanlarda yada binalarda kapsama alanının kontrolü, amaçlanan kapsama alanını oluşturma konusunda yardım eder. Ayrıca erişim noktası kapsama alanının kontrolü için yönlü antenler (directional antenna) kullanır. Yönlü antenler, herhangi bir koruma sağlamazlar. Sadece kapsama alanını kontrol etmeye yardımcı olur.

Kapsama alanının sınırlandırılmasının ve kontrolünün güvenlik anlamında bazı avantajlar getirsede, gerçek bir çözüm olarak görülmemelidir. Çünkü yüksek

kazançlı bir antenle kablosuz ağ trafiğinin dinlenmesi olasıdır. Dolayısıyla kriptografik yöntemlerin kullanılması kaçınılmazdır.

5.3. Teknik Olarak Alınacak Önlemler

Güvenli kablosuz alan oluşturmak için teknik olarak alınacak önlemler donanım ve yazılım çözümleri olarak incelenebilir. Yazılım çözümleri erişim noktasının doğru konfigürasyonunu, yazılım yamalarını ve güncellemelerini, kimlik doğrulamayı, izinsiz girişleri algılama sistemini (intrusion detecetion systems, IDS) ve şifrelemeyi kapsamaktadır. Donanım çözümleri ise akıllı kartlar (smart card), VPN bağlantı, açık şifreleme düzeni (public key infrastructure, PKI) ve biyometrik cihazları içerir.

5.3.1. Yazılım Çözümleri

Yazılım çözümleri, kimlik doğrulamanın kullanılması, erişim noktasının konfigürasyonunun doğru yapılmasını, kimlik doğrulama ve IDS kullanımının yanısıra, güvenlik denetlemelerinin yapılarak gözden geçirme ve etkili bir şifreleme yönteminin kullanılması olarak belirtilebilir.

Erişim Noktasının Konfigürasyonu :

Ağ yöneticileri, belirlenen güvenlik politikasıyla uyumlu olacak şekilde erişim noktalarının konfigürasyonunu yapmalıdır. Doğru bir şekilde konfigürasyonu yapılan yönetici şifreleri, şifreleme ayarları, ilk duruma döndürme (reset) fonksiyonu, otomatik ağ bağlantı fonksiyonu, Ethernet MAC Erişim Kontrol Listesi (Access Control List), ortak anahtarlar ve Ağ Yönetim Protokolü (Simple Network Management Protocol SNMP) üstlenicisi, erişim noktalarının varolan konfigürasyon ayarlarından kaynaklanan saldırıya açık noktaların giderilmesine yardımcı olur.[20]

- Varolan Başlangıç Şifrelerini Güncelleme: Tüm WLAN aygıtları kendilerine ait varolan ayarlara sahip olarak sunulmaktadır. Örneğin bu ayarlardan biri yönetici

şifresidir. Üretilen cihazların pek çoğunun fabrika çıkışı şifreleri aynıdır yada bazı erişim noktalarının fabrika çıkışında şifreleri bile yoktur. Eğer şifre koruması yoksa, yetkisiz kişilerin kolayca ağ kaynaklarına erişimi mümkündür. Ağ yöneticileri varolan başlangıç şifrelerinin değiştirilmesi ve şifrelerde hem alfanumerik hemde özel karekterlerin kullanılmasını sağlayacak güvenlik kuralları (security policy) oluşturmalıdır. Eğer güvenliğin çok daha iyi olması gerekiyorsa, otomatik şifre üreticisi de kullanılabilir. Şifre doğrulanması için diğer bir şecenek, iki faktörlü doğrulamadır. İki faktörlü doğrulamanın bir formu, her dakika yeni bir kod üretmek için simetrik anahtar algoritması kullanır. Kimlik doğrulaması için kişisel tanımlama numarası (PIN – Personnel Identification Number) ile birleşen bu kod bir defaya mahsus olarak kullanılır. İki faktörlü kimlik doğrulamanın diğer bir formu da kullanıcının kişisel tanımlama bilgisi ile akıllı kartların birlikte kullanılmasıdır. Bu tip kimlik doğrulama, akıllı kartlar için bir okuyucu, kişisel tanımlama numarası için de bir doğrulama sunucusu gerektirir. Ticari ürünlerin bir çoğu bu özelliği taşımaktadır. Bununla birlikte, otomatik şifre üreticisi veya iki faktörlü doğrulama mekanizması maliyet, kullanıcı sayısı ve güvenlik isterlerinden dolayı çok da iyi bir yatırım olmayabilir.

- Şifreleme Ayarlarını Uygun Bir Şekilde Yapmak: Tipik olarak, erişim noktalarında birkaç şifreleme seçeneği bulunmaktadır. Bunlar şifreleme kullanmama, 40 bit ortak anahtar ve 104 bit ortak anahtardır. WEP içinde kullanılan şifrelemede, kesintisiz akış şifresi üretme (Stream cipher generation) ve EXOR işlemi bilgisayarın işlemcisine herhangi ek bir yük getirmez. Dolayısıyla şifrelemenin kullanımında ve planlanmasında işlemcinin kullanımı konusuna endişelenmeye gerek yoktur. Bununla birlikte şu konu unutulmamalıdır ki, WEP'e karşı yapılan bazı saldırılar, kullanılan anahtar uzunluğuna rağmen kötü sonuçlar doğurabilir. Ayrıca değinilmesi gereken diğer bir önemli noktada, 128 bitlik anahtarlar kullanan ürünlerle, 104 bitlik anahtar kullanan ürünlerin birlikte çalışamayacağıdır.

- Başlangıç durumuna döndürme fonksiyonunu kontrol etme: Başlangıç durumuna dönme de bir problemdir. Çünkü bu işlem erişim noktasının konfigure edilen tüm ayarlarının iptal olmasına neden olur. Yani erişim noktası fabrika

ayarlarına dönmüş olur. Genellikle fabrika çıkış ayarlarında herhangi bir yönetici şifresi tanımlanmamıştır hatta şifreleme aktif bile olmayabilir. Fiziksel olarak cihaza ulaşabilen kötü niyetli birisi, cihazı resetleyerek cihaz üzerindeki tüm güvenlik önlemlerini iptal edebilir. Reset fonksiyonu IP adresi ve anahtarlar gibi basit operasyonel bilgileri silmek üzere konfigure edildiyse cihazın devre dışı kalmasına da sebep olabilir. Çünkü birçok erişim noktası bu ayarlar olmadan çalışamaz. Dolayısıyla erişim noktalarına fiziksel erişimin kontrol altında tutulmasını sağlanması riskleri azaltmak için az da olsa işe yarayacaktır. Ayrıca düzenli olarak güvenlik denetlemeleri yapılması da risklerin azalmasını sağlayacaktır. Ek olarak, bazı ürünlerin yönetim arabirimleri aracılığıyla cihaza uzaktan erişim mümkün hale gelmektedir. Bu yüzden bu arabirim üzerinde düzgün şifre yönetimine ve veri şifreleme yönteminin kullanımı son derece gereklidir.

- MAC ACL foksiyonunun Kullanımı: MAC adresi ağ üzerindeki her bilgisayarı tanımlayan ve bilgisayara özgü yani tek olan donanım adresidir. Ağlar, aynı altağ üzerinde bulunan bilgisayarlardaki farklı ağ arabirim kartlarının iletişim kurmasını sağlamak için MAC adreslerini kullanır. 802.11 ürünlerinin birçoğu MAC ACL listesine dayalı olarak erişimi kısıtlayan özellikler içerir. MAC ACL, MAC adresine göre düzenlenmiş izin listesini kullanarak bilgisayara erişimi engeller yada erişime izin verir. Bununla birlikte tek başına Ethernet MAC ACL çok güçlü bir savunma mekanizması değildir. Çünkü MAC adresleri kablosuz NIC ‘ten erişim noktasına açık bir şekilde gönderilir ve MAC adresleri çok kolay bir şekilde elegeçirilebilir. Kötü niyetli kullanıcılar kendi MAC adreslerini kablosuz ağa ulaşım hakkı olan başka bir MAC adresi ile değiştirebilir. Dolayısıyla bu önlem belli bir düzeyde güvenlik sağlayabilir. MAC ACL fonksiyonu kasıtlı olmayan hat dinleme ve izlemelere karşı etkili olsada, saldırılara karşı güvenlik önlemi sayılmaz. Ancak yinede güvenlik önlemlerine ek olarak, problem olasılığını azaltmak kullanılabilir. Bununla birlikte bu önlemi kullanacak organizasyonların MAC ACL fonksiyonunu aktif hale getirme konusunda yaşanacak yönetimsel iş yükünü de göze almaları gerekir. Ek olarak, bir çok ürün MAC ACL için sınırlı sayıda MAC adresini destekler. Dolayısıyla orta ve büyük ölçekli ağlarda, sınırlı sayıda MAC adresi içerebilen erişim kontrol listesinin büyüklüğü yeterli olmayabilir. [8]

- SSID’nin Değiştirilmesi: Erişim noktasının fabrika çıkışında varolan başlangıç SSID numarası değiştirilmelidir. Çünkü birçok 802.11 kablosuz LAN üreticisinin kullandığı başlangıç SSID değeri yayınlanmaktar ve dolayısıyla herkes tarafından da bu numaralar bilinmektedir. Kolay bir şekilde erişimi engellemek için bu değer değiştirilmelidir. Buna rağmen donanımlı birisi tarafından, kablosuz arabirim üzerinden bu tanımlayıcı parametre ele geçirilebilir.

- İşaret Işığı (Beacon) aralığını artırmak: 802.11 standardı, kablosuz ağın varlığını gösteren işaret ışığı karelerinin (Beacon frames) kullanımını tanımlar. Bu işaret ışıkları erişim noktasından belirli zaman aralıkları ile gönderilir ve kablosuz ağa bağlanması için istasyonun konfigürasyon parametrelerini eşleştirmesine ve tanıtmasına izin verir. Erişim noktaları Beacon karelerinin ve onun zorunlu SSID alanının gizlenmesini sağlayacak şekilde konfigure edilmemiştir. Bununla birlikte, bu işaret ışığının zaman aralıkları en yüksek değeri olan 67 dakikaya ayarlanabilir. Böylece ağı bulmak zorlaşır. Çünkü deyim yerindeyse erişim noktası daha sessiz olur ve SSID sık sık gönderilmemiş olur. Dolayısıyla kablosuz ağların uzun işaret ışık aralıklarıyla konfigüre edilmesi gerekir.

- SSID ‘nin yayınlanmaması : SSID, ağ ismi olarak da adlandırılabilen bir tanımlayıcıdır ve basit ASCII karekterlerinden oluşmaktadır. SSID kablosuz ağa tanımlayıcı atamak için kullanılır. Ağa bağlanmak isteyen istasyonlar bağlanabilecekleri ağlar için alanı tararlar ve doğru SSID bulduklarında bağlanırlar. SSID 0-32 bayt aralığında boşluk-sonlandırmalı (null-terminated) ASCII dizisidir. Bu dizideki sıfır baytı özel bir durumu gösterir ve SSID’nin yayımlanması ile ilgilidir. Kablosuz istasyonlar, bir alan içerisinde aktif olarak erişim noktalarını tarayarak bu alandaki tüm ağları tespit ederler. Bu işlem sırasında yayımlanan Probe İstek mesajını kullanırlar. Bu isteği alan SSID’si yayınlanan tüm 802.11 ağları Probe cevap mesajı gönderirler. Erişim noktalarında SSID’nin yayınlanmasını engellemek, erşim noktasının kendisine gelen istasyon isteklerini yok sayması anlamına gelir ve böylece aktif yani özel SSID numarası ile tarama yapılması zorunlu hale gelir.

- Varolan Kriptografik Anahtarların Değiştirilmesi: Kablosuz ağ cihaz üreticileri, ağa ulaşmak isteyen cihaz ve erişim noktası arasında ortak anahtar kimlik

doğrulamasını aktif hale getirmek için bir yada bir kaç anahtar sunarlar. Varolan bu ortak anahtarları kullanmak güvenlik açığıdır. Çünkü pek çok üretici fabrika çıkışında ürünlerinde belirli ortak anahtarları kullanırlar. Herkes tarafından bilinmesi ve bulunması mümkün olan bu ortak anahtarlar herkesin ağa erişebilmesini mümkün kılmaktadır. Dolayısıyla varolan bu anahtarların değiştirilmesi riski azaltacaktır. Riski azaltmanın diğer bir yolu uzun anahtarlardır. Bunun dışında anahtar yönetimi konusunda genel olarak kabul edilmiş başka bir prensipte, anahtarların sık sık değiştirilmesi ve personel değişikliklerinde de anahtarların değiştirilmesidir.

- SNMP (Simple Network Management Protocol – Basit Ağ Yönetim Protokolü) Kullanımı: SNMP, ağ cihazlarında yönetimsel bilgi alışverişinin sağlanması için oluşturulmuş bir uygulama katmanı protokolüdür. TCP/IP protokolünün bir parçası olan SNMP, ağ yöneticilerinin ağ performansını arttırması, ağ problemlerini bulup çözmesi ve ağlardaki genişleme için planlama yapabilmesine olanak sağlar. Kablosuz erişim noktalarının bazıları SNMP Üstlenici kullanırlar. SNMP Üstlenici, ağ yönetimi araçlarının, kablosuz erişim noktası ve istasyonun durumlarını izlemesine izin verir. SNMP'nn ilk iki yani SNMP, SNMPv1 versiyonları şifresiz belge dizisine dayalı olarak sadece açık kimlik doğrulama yöntemini desteklediğinden güvenli değildi. SNMP'nin üçüncü versiyonu ise yüksek güvenlik ihtiyaçlarını sağlayacak mekanizma içermektedir. Eğer ağ üzerinde SNMP kullanılmayacaksa, devre dışı bırakılabilir. Ancak versiyon 3'ün dışındakiler kullanılacaksa bazı riskleri göze almak gerekecektir. Çünkü genellikle SNMP üstlenicilerinin kullanmış olduğu varolan SNMP dizisi "public" kelimesidir ve okuma veya hem okuma hem yazma hakları atanmıştır. Bilinen bu varolan diziyi kullanmak aygıtları saldırıya açık hale getirmeye neden olmaktadır. Eğer yetkisiz bir kullanıcı okuma yazma hakkıyla kaynaklara ulaşırlarsa, verileri değiştirebilirler ve buda veri bütünlüğünün kırılması anlamına gelmektedir. Dolayısıyla SNMP'nin kullanılması gereken yerlerde bu dizinin değiştirilmesi gerekmektedir. İzinler ise sadece okunabilir şekilde ayarlanmalıdır. Güvenlik sebebiyle SNMPv1 ve SNMPv2 yerine SNMPv3 tercih edilmelidir.

- Varolan kanalı değiştirilmesi: Üreticiler genellikle erişim noktalarında varolan kanalları kullanırlar. Varolan bu kanalları kullanan iki veya daha fazla erişim noktası birbirlerine yakın olduklarında ve farklı ağlarda bulunmaları durumunda sistemin servis dışı kalmasına sebep olurlar. Yani iki erişim noktası arasındaki radyo dalgalarının girişiminden dolayı erişim noktaları hizmet dışı kalabilirler. Dolayısıyla radyo dalgalarının girişimine maruz kalmamak için yanyana yakın duran erişim noktalarının farklı aralıktaki kanalları kullanmaları sağlanmalıdır. Örneğin, kanal1, 6 ve 11 aynı anda erişim noktaları tarafından herhangi bir radyo sinyalleri girişimine neden olmadan kullanılabilir. Ayrıca alan içindeki tüm kaynakların radyo girişimlerine bakılmalı ve alan incelemesi yapılmalıdır. Alan incelenmesinde ortaya çıkan raporda kapsama alanları belirlenmesi, erişim noktasının yerleştirileceği yerler ve erişim noktalarına atanan radyo kanalları bulunmalıdır.

- DHCP (Dynamic Host Control Protocol – Dinamik İstemci Ayarlama Protokolü) Kullanımı: DHCP sunucuları, bir altağdan diğerine geçerken erişim noktasına bağlanmaya çalışan cihazlara otomatik olarak IP adresi atamak için kullanılır. Örneğin, DHCP sunucu dizüstü yada masaüstü bilgisayarlar için TCP/IP adres aralığını belirlemek ve yönetmek amacıyla kullanılır. IP adres aralığı belirlendikten sonra DHCP sunucu, isteyen istasyonlara dinamik olarak IP adresi atar. Bu sunucu, WLAN'nın şifreleme ayarlarına uygun şekilde cihazla dinamik IP adresi atar. DHCP kullanımı ile ilgili risk şudur. Herhangi bir kullanıcı, kablosuz arabirim kartına sahip bir dizüstü bilgisayarla çok kolay bir şekilde yetkisi olmasada ağa girebilir. DHCP sunucu hangi kablosuz cihaza IP verip vermeyeceğini bilmediğinden otomatik olarak istekte bulunan her bilgisayara IP adresi vermektedir. Bu konudaki riskleri azaltmak için mümkünse DHCP sunucu kullanmak yerine, statik IP adresleri kullanmak daha doğru olur. Ancak bu alternatif MAC ACL önleminde olduğu gibi sadece küçük ağlarda pratik olabilir. Statik IP verme ağ ve sistem yöneticilerinin iş yükünü artırdığı gibi, kablosuz ağların bazı anahtar avantajlarını örneğin dolaşımı (roaming) yada eşler arası (ad hoc) ağ kurulumunuda engellemiş olur. Diğer çözümde erişim noktalarıyla birleştirilmiş ateşduvarlarının kullanımıdır. Bu son çözümde tüm ağa ek bir koruma katmanı eklenecektir.

Yazılım yamaları ve güncellemeleri:

Ağ yöneticileri düzenli olarak kullandıkları ürünlerin güvenlik yamaları ve güncellemeleri olup olmadığı kontrol etmeli ve varsa gerekli çalışmayı yapmalıdır. Ayrıca üretici firmalar müşterilerini bu konuda yeni güvenlik açıkları ve saldırıları ile ilgili olarak e-posta aracılığıyla uyarmaktadır. Ayrıca ağ yöneticileri, yayınlanan yazılım ve donanımla ilgili güncellemeleri ve yamaları kontrol ederek gerekli çalışmaları yapmalıdır.

- Kimlik Asıllama: Genel olarak, ağa sadece yetkili kişilerin girmesine izin vermenin en güvenilir yolu etkili bir kimlik doğrulama çözümüdür. Kimlik doğrulama çözümlerine kullanıcı adı ve şifre kullanımı; akıllı kartlar, biyometrik çözümler, PKI yada bu çözümlerin birlikte kullanılması örnek verilebilir. Kimlik doğrulama kullanıcı adı ve şifre kullanımına dayalı olarak yapıldığında, bazı kurallara uyulması güvenlik açısından önemlidir. Örneğin bu kurallarda en düşük şifre uzunlukları, şifrelerde kullanılması gereken karekterler ve şifrelerin zamanın dolması gibi özellikler tanımlanmalıdır.

Organizasyonlar gereken güvenlik düzeyine ve veri gizlilik gerekliliğine bakılmaksızın, güçlü bir şifreleme politikasının uygulanması sağlamalıdır. Kullanılan şifrelerin güçlü tahmin edilemez olması her ortam için en temel güvenlik ölçütüdür. Bunun yanısıra gerekiyorsa diğer kimlik doğrulama yöntemleri yani PKI, biyometrik cihazlar yada akıllı kartları kullanmalıdır. Çünkü bu mekanizların WLAN ile birlikte kullanımı güvenliğin artması anlamına gelmektedir. Aynı zamanda kullanıcılarında geliştirilmiş kimlik doğrulama ile sağlanan güvenliği tam anlamıyla anlayıp dikkat etmeleri gerekir. Örneğin çok güçlü bir şifre sistemi WEP ‘in kriptografik problemlerini ortadan kaldırmayacaktır.

- Kişisel Ateşduvarları :Kablosuz ağ üzerindeki herkese açık kaynaklar, büyük saldırı riski altındadır. Kişisel ateşduvarları, bazı saldırılara karşı koruma sağlayabilmektedir. Kişisel ateşduvarları, yazılım tabanlı ve istasyon tarafında bulunan çözümlerdir. Bu yazılım kullanıcı tarafından yönetilebileceği gibi merkezi

bir şekilde de yönetilebilir. İstasyon tarafında yönetilenlerde tüm konfigürasyonlar kullanıcı tarafından yapıldığından kullanımı daha uygun olabilir. Ancak merkez tarafından yönetilen versiyonlarında, tüm konfigürasyon bir IT ekibi tarafından ve uzaktan yapıldığından daha iyi koruma sağlayabilmektedir. Merkezden yönetilen çözümler organizasyonlara, saldırılara açık noktaların korunabilmesi için istasyonda gerekli değişikliklerin merkezden yapılma imkanını sağladığı gibi, tüm uzaktan bağlı kullanıcılar için ağın güvenlik politikasının sürdürülebilmesini sağlar. Kişisel ateşduvarları bir miktar koruma sağlasa da, gelişmiş saldırılara karşı koruma sağlamamaktadır. Güvenlik gereksinimlerine bağlı olarak, organizasyonlar güvenlik için ektra katmanlara ihitiyaç duyabilir. Herkese açık olan kablosuz ağlara erişen kullancılar kişisel ateşduvarları kullanmalıdırlar. Kişisel ateşduvarları bunun yanısıra herkese açık yerlerdeki kablosuz ağlara kötü amaçlı olarak yerleştirilmiş erişim noktalarına karşı da koruma sağlamaktadır. [20]

- Saldırı Algılama Sistemi (IDS – Intrusion Detection System):Saldırı algılama sistemi, herhangi bir şekilde ağa izinsiz girmeyi deneyen, izinsiz bir şekilde girmiş yada sistemi tehlikeye atmış herhangi bir durumun bulunup bulunmadığını tespit etmek için kullanılan etkili araçlardır. WLAN sistemler için kullanılan IDS'ler ana bilgisayar-tabanlı, ağ-tabanlı yada her ikisinin özelliklerini kullanan hibrit tabanlı olabilemektedir. Bilgisayar tabanlı IDS, saldırıya açık sistemlere ek bir koruma katmanı getirmektedir. Bilgisayar tabanlı IDS üstlenici, veritabanı sunucusu gibi bir sistem üzerine kurulur ve şüpheli kullanımlar için sistem günlüklerini ve denetlemelerini izler. Örneğin tekrar eden ve başarısızlıkla sonuçlanan sisteme giriş denemelerini veya dosya izinlerinin değişimlerini izler. Bu üstlenici aynı zamanda, doğruluk tablolarına bakarak belirli aralıklarla sistem dosyalarındaki değişiklikleri izler. Bu üstlenicinin ilk görevi olayları analiz etmesi, alarm mesajı göndermesi ve günlükleri incelemesi olmasına rağmen, bazı saldırılar karşısında sistemi durdurabilir. Ağ-tabanlı IDS'ler ise gerçek zamanda LAN trafiğini paket paket izleyerek, herhangi bir şekilde saldırıyla ilgili bir gösterge ipucu var mı yok mu diye kontrol eder. Örneğin DOS saldırıları hedef sisteme parçalara ayrılmış paketler gönderir. Ağ izleyici bu tip saldırı paketlerine benzeyenleri tanıyarak, sistem yöneticisine bir alarm e-postası gönderir, o andaki ağ oturumunu durdurur yada

belirlenmiş hangi aksiyon varsa gereğini yerine getirir. Bilgisayar tabanlı IDS sistemler, ağ tabanlı olanlara göre biraz daha avantajlıdır. Çünkü üstlenicinin kendisinde bulunmasından dolayı bilgisayar tabanlı sistem, verinin şifresi çözüldükten sonra veriyi inceleyebilir. Halbuki ağ tabanlı sistemde, verinin şifresi çözülmez. Bu yüzden şifreli ağ trafiği herhangi bir incelemeye tabi tutulmadan geçer. [29]

Kablolu ağ üzerindeki IDS sistemi, kablosuz ağı korumak için kullanıldığında bazı kısıtlamalara sebep olmaktadır.

Kablosuz erişim noktasının gerisinde kablolu ağ üzerindeki ağ-tabanlı IDS sensörleri, aynı altağ üzerindeki bir kablosuz istasyondan bir başka istasyona yapılan saldırıları yakalayamaz. Kablosuz erişim noktası, trafiği kablosuz istasyonlar arasında değiştirmektedir. Trafik kablolu ağa girmez, WEP şifreli verileri kablolu ağ IDS sensörleri analiz edemez. Sonuç olarak, yetkisi olmayan bir kablosuz istasyon ağa giriş yaparak, ağ-tabanlı IDS sensöre yakalanmadan diğer kablosuz bilgisayarlara saldırabilir. [29]

Kablolu ağ üzerindeki IDS sensörleri, genellikle yetkili yasal bir istasyonun kablosuz ağ ile ilişkisinin bitmesini algılamaz. Ayrıca, yetkisi olmayan kablosuz kullanıcının kablosuz ağ ile olan ilişkisini de algılamaz. Kablosuz cihazlara karşı yapılan saldırılar fiziksel ve veri-bağlantı katmanı tekniklerini kullanırlar. IDS sensörler bu teknikle yapılan saldırıları tanımaz.[30]

Kablolu ağlardaki IDS teknoloji, sadece kablosuz istasyondan kablolu ağ üzerindeki bir bilgisayara yapılan saldırıları algılayabilir. Bu noktada kablosuz ağ risk altınadır. Dolayısıyla aynı risk kablolu ağ için de söz konusudur. Buradaki hedef kablolu ağları etkilemeden önce, yetkisiz kablosuz aktivitelerinin algılanması ve alarm gönderilmesidir. [30]

Kablolu ağ üzerindeki IDS teknoloji bina içerisindeki sahte erişim noktalarının yerini tespit edemez. Bu sahte erişim noktaları, uzak bir lokasyondan, yetkisiz kablosuz erişim için giriş noktası olacaktır.

IDS teknoloji, yetkili bir kablosuz cihazın, yetkisiz bir kablosuz cihazla eşten eşe iletişimlerini de algılayamaz. Burada oluşan eşten eşe mod dolayısıyla kablolu ağa bir köprü kurulmuş olur ve dolayısıyla saldırılar kaçınılmaz olur.

Bir yada daha fazla kablosuz ağı kablolu ağ ile genişletmek, ağ güvenliğini sağlamak için bir çok önlem alınmasını beraberinde getirir. Kablolu ağ üzerindeki IDS sensörlerin algılayamayacağı riskler ortaya çıkar. Dolayısıyla kablolu ağı kablosuz ağ ile genişletmek isteyen organizasyonlar, varolan IDS sistemlerini gözden geçirmeli ve kablosuz IDS sistemleri sisteme entegre etmelidirler.[30]

Kablosuz IDS sistemlerin özellikleri :

Bina içinde yada çevresindeki kablosuz cihazın fiziksel olarak bulunduğu yeri tanımlayabilir.

Kablolu ağ tarafında görülmeyen, kablosuz ağdaki yetkisiz eşten eşe bağlantıları algılar.

Kablosuz iletişimi analiz ederek, 802.11 RF alanını izler. Güvenlik kurallarını ihlal eden kablosuz cihazlardaki yetkisiz bir şekilde yapılan konfigürasyon değişikliklerini algıladığında alarm üretir.

Sahte erişim noktalarını algılar.

Merkezi izleme ve yönetim özelliklerinin varolan IDS izleme ve raporlama yazılımı ile birleştirilmesi, kablosuz ve kablolu ağın güvenliğinin bir arada izlenmesini sağlayacaktır.

Yüksek düzeyde güvenlik gereken sistemlerde IDS kullanılmalıdır. Çünkü bu yapı güvenlik açısından sisteme ek bir katman getirmektedir.

- Şifreleme:Kablosuz ağlardan ilk söz edilmeye başlandığı zamanlarda, erişim noktaları için sadece üç şifreleme seçeneğinden bahsediliyordu. Bunlar şifresiz, 40 bit ortak anahtar ve 104 bit ayarlarıdır. Bu seçeneklerden None seçeneği, ağ açısından çok büyük risk anlamına gelmektedir. Çünkü ağ üzerindeki şifrelenmemiş veri kolay bir şekilde ele geçirilebilir, okunabilir ve değiştirilebilir. 40 bit ortak anahtar kullanımı seçeneği ise verinin şifrelenmesini sağlar ancak yine de risk devam etmektedir. Çünkü 40 bitlik şifreleme yüksek teknolojiye sahip, bazen çok yüksek teknolojiye sahip olmayan bilgisayarla bile kırılabilmektedir. Bu seçenekler arasında en iyisi 104 bitlik şifrelemedir. Bu seçenekte kullanılan anahtar boyutu 40 bitten büyük olduğundan kırılması daha zordur. Ancak 802.11 WEP için kullanılan başlangıç vektörünün zayıf kriptografik yapısından dolayı WEP şifrelemenin çok güvenli olduğu söylenilemez. Tekrar belirtmek gerekirse, WEP protokolündeki güvenlik problemlerinin üstesinden gelmek için, 802.11 kullanıcıları, erişim noktaları ve istasyonlar için çıkan yazılım yamalarını zaman zaman kontrol ederek, gerekli güncellemeleri yapma konusunda tedbirli, özenli ve dikkatli olmalıdır.

- Güvenliği Değerlendirme: Güvenlik değerlendirmesi yada denetlemesi, kablosuz ağın güvenlikle ilgili durumunu kontrol etmek ve güvenliğin devamını sağlamak için temel bir araçtır. Sistemin, kablosuz ağ çözümleyici yada benzeri araçlarla belirli aralıklarla denetlenmesi önemlidir. Bu güvenliğin sağlanması için gerekli çalışmaların yapılmasını sağlar. İzci (sniffer) olarak da adlandırılan çözümleyiciler, güvenliğin denetlemesi ve kablosuz ağ arızaları konularında etkili araçlardır. Güvenlik yöneticileri yada denetçileri, kablosuz ürünlerin doğru bir şekilde iletimi gerçekleştirip gerçekleştirmediğini, doğru kanalı kullanıp kullanmadığını tespit etmek için ağ çözümleyici araçları kullanabilir. Ayrıca ağ yöneticileri, herhangi bir sahte ve gizli erişim noktasının yerleştirilip yerleştirilmediğini anlamak için periyodik olarak ofis binalarını, kampüslerini kontrol etmelidir. Ayrıca ağ yöneticileri, üçüncü tür araçlarda kullanarak güvenlik denetlemeleri yapmalıdır. Bu üçüncü tür çözümler, izinsiz girişleri tespit edebilir. Organizasyonlara,kablosuz ağlarının hazırlanan güvenlik prosedürleri ve politikası

ile uyumlu olup olmadığı konusunda yardım eder. Ayrıca sistemleri yeni güncellemeler ve yamalarla güncel tutar.

5.3.2. Donanım Çözümleri

WLAN'ların karşı karşıya kaldıkları riskleri azaltmak için alınabilecek donanım çözümleri akıllı kartlar, biyometrik cihazlar, VPN'ler, PKI ve diğer donanım çözümleridir.

- Akıllı Kartlar : Akıllı kartlar sistemin kompleks yapısına yeni bir katman eklemiş olmasına rağmen, risklere karşı sistemi korumaktadır. Akıllı kartlar iki-faktör kimlik doğrulamada kullanılır. Ayrıca biyometrik cihazları ile birlikte kullanılması mümkündür. Kablosuz ağlarda, akıllı kartlar kimlik doğrulamaya ek özellik getirmektedir. Akıllı kartlar kullanıcı adı ve şifrenin yanında kimlik doğrulama için ek özellikler istenen sistemlerde yararlıdır. Kullanıcı sertifikaları ve diğer bilgiler akıllı kartlara yüklenir ve genellikle kullanıcının PIN numarasını hatırlaması yeterlidir. Akıllı kartlar taşınabilir de olduğundan, kullanıcılar değişik yerlerden güvenli bir şekilde ağlarına erişebilirler. [20]

- Sanal Özel Ağ : Sanal Özel Ağlar, herkese için açık ağ yapısında güvenli veri iletimi sağlayan ve son yıllarda gelişmiş bir teknolojidir. Günümüzde bu ağlar; ağa uzaktan erişim için, LAN'lar arasında bağlantı kurmak için ve dış internet olmak üzere üç farklı şekilde kullanılır. VPN'ler IP bilgisini korumak için kriptografik teknikler kullanırlar. VPN tunelindeki veri şifrelenmiştir ve diğer ağ trafiklerinden izole edilmiştir. İki site arasındaki VPN bağlantısını Şekil 5.1. üzerinden incelemek mümkündür. Bu yapıda, site A'dan site B'ye iletişim internet üzerinden olsa bile korumalıdır ve veri bütünlüğü, gizliliği ve diğer güvenlik servisleri sağlanmaktadır.[25]

Günümüzde kullanılan VPN bağlantıda çoğunlukla IPsec protokolü kullanılmaktadır. IPsec, IETF (Internet Engineering Task Force) tarafından geliştirilen bir protokoldür ve IP ağlar üzerinden özel iletişim kurma imkanı sağlarlar. IPsec protokolünü, güvensiz bir ortamda iki kişinin güvenli bir şekilde

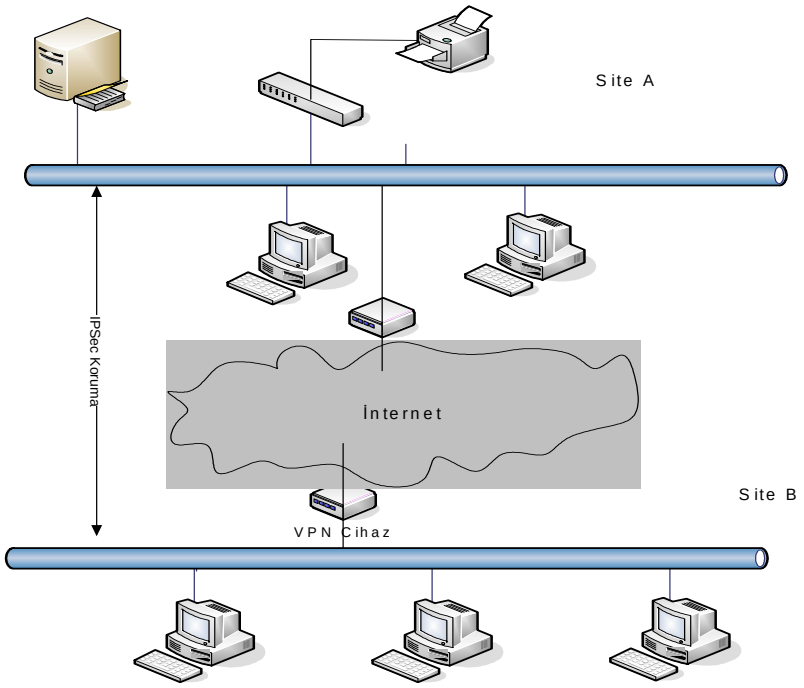
konuşmasını sağlamak, bu konuşma sırasında her iki kişinin gerçekten doğru kişiler olmasının sağlanması ve ilgili konuşmanın 3. bir kişi tarafından dinlenmemesini/değiştirilmemesini sağlamak olarak da tanımlanabilir. [20]

IPSEC tanım olarak IP katmanında tüm IP iletişimini şifrelemek ve doğrulamak için kullanılan bir standarttır.

IPSEC iki şekilde karşımıza çıkar; ESP ve AH

ESP :Encapsulation Security Payload Doğrulama, bütünlük-değiştirilmeme ve güvenilirlik işlemlerinin tümünü gerçekleştirmektedir.

AH :Kimlik Doğrulama Başlığı (Authentication Header) adından da anlaşılabileceği gibi sadece doğrulama ve bütünlük-değiştirilmeme işlemlerini sağlamakta fakat güvenilirliği yerine getirememektedir. [28]

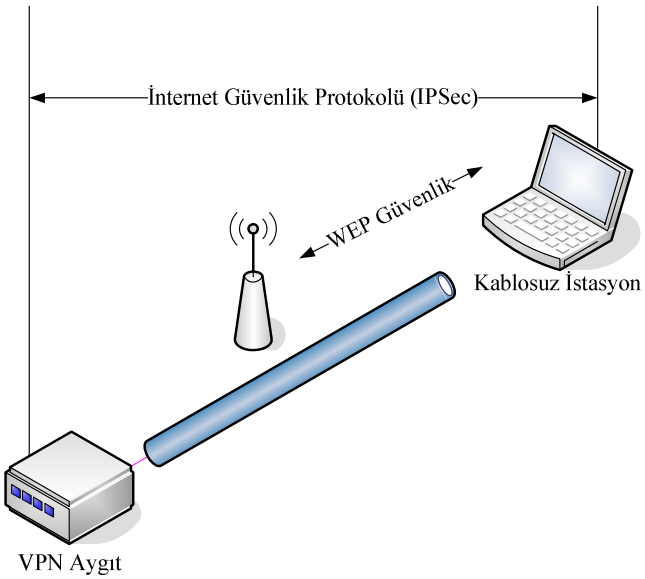


Şekil 5.1. Siteler arası Güvenli İnternet İletişimde VPN Kullanımı [20]

AH’ nin ESP’ ye göre bir artısı vardır o da AH’ nin IP Başlık bilgisini de doğrulayabilmesidir.

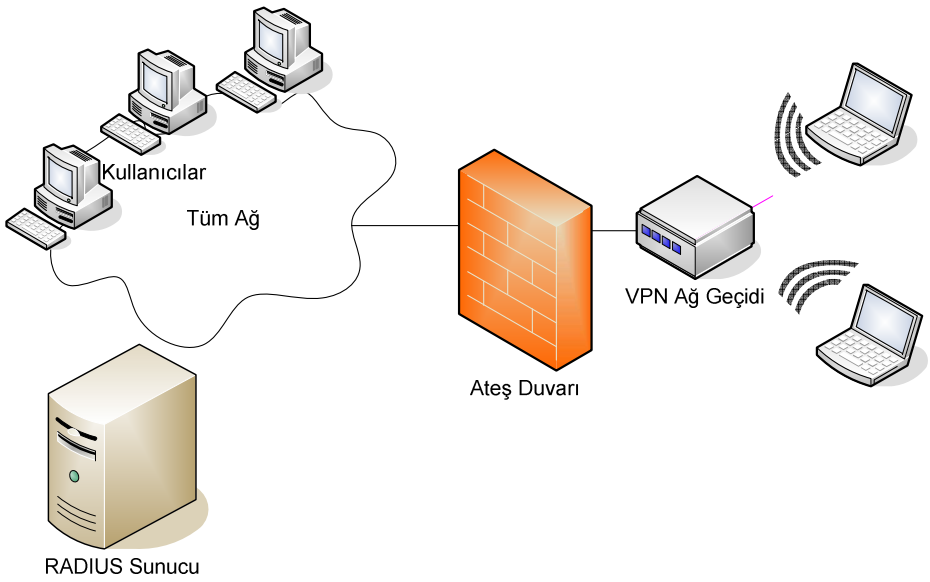
Burada sözü geçen doğrulama(authentication), her iki kişinin gerçekten doğru kişiler olması; bütünlük-değistirilememe (data integrity), konuşmanin içeriğinin değişmeden karşıya ulaşması; güvenilirlik (confidentiality/encryption) konuşmanın 3. bir kişi tarafından duyulsa bile anlaşılmaması anlamına gelmektedir. [28]

WLAN sistemlerde IPsec kullanımı ile ilgili olarak Şekil 5.2.’de kablosuz istasyondan erişim noktasına ve sanal özel ağ aracına IPsec tüneli sağlanmıştır. IPsec kullanımı ile güvenlik servisleri, ağ katmanından sağlanmaktadır. Bunun anlamı, bu katman üzerindeki tüm uygulama ve protokollerin IPsec ile korunmasıdır. IPsec güvenlik servisleri, katman 2 ‘deki güvenlikten yani WEP güvenliğinden bağımsızdır. Sonuç olarak, eğer VPN kullanılacaksa, IPsec ve WEP birlikte kullanılmalıdır. Aşağıdaki şekilde görüldüğü üzere, VPN kablolu ağdan gelen giden verileri şifrelemektedir. [28]



Şekil 5.2. WEP protokolünün VPN yapıda kullanımı [20]

Şekil 5.3. kablosuz ağlarda VPN kullanımının diğer bir örneğidir. Şekilde de görüldüğü gibi, kablosuz cihazlar ve VPN ile istasyonlar güvenli bir şekilde VPN geçitinden (gateway) ağa bağlanırlar. Kablosuz istasyonlar, kablosuz VPN geçiti ile WEP'in yerine yada ek olarak IPsec bağlantısı kurar. Burada istasyonların herhangi ek bir donanıma ihtiyacı yoktur. Sadece IPsec/VPN yazılımının kurulması yeterlidir. VPN geçiti, kablosuz istasyon cihazının doğrulanması için paylaşılmış kriptografik anahtar veya dijital sertifika kullanabilir. VPN çözümü için önceden paylaşılmış anahtar kullanımı organizasyonları, WEP'te olduğu gibi anahtar dağıtım problemlerini ve aynı özellikleri beraberinde getirir. VPN geçitinde kullanıcı doğrulaması, RADIUS sunucu yada bir kez kullanımlık şifre (one-time-password) kullanılarak yapılabilir. Günümüzde kullanılan VPN geçitlerinin birçoğu ağ üzerinde giden gelen verileri ve izinsiz erişimlere karşı ağı korumak için ateşduvarı özelliği ile birlikte gelir. Aynı zamanda VPN geçitinin ateşduvarı özelliği hem maliyet hem de yönetim yükü açısından avantajlıdır. Ayrıca Ateşduvarlı VPN geçitlerinin, tüm aktiviteleri tutan günlük özelliğine de içerenleri vardır. Güvenlik yöneticisi, VPN geçiti üzerindeki bu günlüğü kullanarak güvenliği denetleyebilir ve girenlerin kimliği doğrulanmış kişiler mi yoksa izinsiz kullanıcılar mı olduğunu görür. [25]



Şekil 5.3. Basitleştirilmiş VPN WLAN Diyagramı [20]

VPN kullanımı her ne kadar hava ortamında güvenliği artırıyor gibi olsa da bu yaklaşım tüm ağ için tam bir güvenlik sağlamaz. Örneğin, bu çözüm ağda çalışan uygulamalar için kimlik doğrulama ve yetkilendirme işlemleri ile ilgili tam güvenlik sağlamaz.

- Açık Anahtar Altyapısı (PKI) :PKI uygulamalarında her kullanıcının biri özel diğeri genel olmak üzere iki anahtarı bulunur. Kullanıcının genel anahtarı herkese açık olup, özel anahtarı yalnız ve yalnız kullanıcının kendisi (kullanıcı uygulaması) tarafından bilinir. Özel ve genel anahtar arasında çözülmesi pratikte imkansız bir matematiksel ilişki vardır ki kullanıcının genel anahtarı ile şifrelenen bir mesaj yalnız ve yalnız aynı kullanıcının özel anahtarı ile deşifre edilebilir. Bunun tersi de doğrudur, yani kullanıcının özel anahtarı ile şifrelenen bir mesaj ancak aynı kullanıcının genel anahtarı ile deşifre edilebilir. Dolayısıyla bir kullanıcıya şifreli bir mesaj göndermek istendiğinde mesaj bu kullanıcının genel anahtarı ile şifrelenebilir ve böylece mesaj gerçek alıcısı dışında kimse tarafından deşifre edilemez. [5]

Kullanıcının genel anahtarının gerçekten o kullanıcıya ait olduğundan nasıl sertifika otoriteleri (CA - Certificate Authority) sayesinde emin olunur. Bir PKI sisteminde, tüm kullanıcıların tanıdığı (güvendiği) ve genel anahtarı tüm kullanıcılar (uygulamalar) tarafından bilinen bir sertifika otoritesi bulunur. Kullanıcıların genel anahtarları, sertifika otoritesinin güvencesi altındadır ve tüm genel anahtarlar sertifika otoritesi tarafından imzalanmıştır. [26]

Dijital imza çok temel olarak her iki parti (gönderen – alıcı) tarafından bilinen bir verinin, gönderen tarafın özel anahtarı ile şifrelenmesi ile elde edilir. Alıcı taraf, gönderenin genel anahtarı ile deşifre ettiği verinin doğrulamasını yaparak imzanın gönderen tarafa ait olduğundan emin olur. Sertifika otoritesinin genel anahtarları imzalaması da bu şekilde olur.

Örneğin A kişisinin, B kişisine bir şifreli mesaj göndermek istediğini varsayalım. Oturum, B'nin genel anahtarını sertifika otoritesinden doğrulayan A'nın, B'ye bu anahtarı kullanarak oturum açma istemini ve oturum anahtarının bir kısmını

oluşturacak mesaj parçasını göndermesi ile başlar. B kişisi, bu mesaj parçasını kendi özel anahtarı ile deşifre ederek, yine oturum anahtarının bir kısmını oluşturacak mesaj parçasını da içeren cevabını, A'nin genel anahtarı ile şifreleyerek A'ye gönderir. Böylece her iki taraf o oturumda kullanılacak oturum anahtarı üzerinde anlaşmış olur. A göndermek istediği mesajı bu oturum anahtarı ile şifreleyerek B'ye gönderir. [20]

B'nin, bu mesajın gerçekten A'dan geldiğinden emin olması için şu işlemler gerçekleşir. A, mesajın sonuna mesajın tümünden özel bir algoritma ile elde edilen bir özütü (digest) kendi özel anahtarı ile şifreleyerek ekler. B, bu imzayı A'nın genel anahtarını kullanarak deşifre eder ve aldığı mesajdan aynı algoritmayı kullanarak elde ettiği özüt ile karşılaştırır. Eğer bir farklılık var ise mesajın A'dan gelmediği veya iletim sırasında değiştirilmiş olduğu ortaya çıkmış olur. [20]

Kablosuz sistemlere, kimlik doğrulama için PKI entegre edilerek, daha güvenli bir ağ oluşturulmuş olur. Günümüzde kablosuz PKI, akıllı kart vb. kablosuz ağlara entegre edilerek kullanılmaktadır.

Buradaki kablosuz bütünlük, alınan mesajın herhangi bir şekilde orjinalinden farklı olmaması yani değiştirilmemiş olmasıdır. Veri merkezli kimlik doğrulama, alınan mesajın gerçekten gönderen kişi tarafından geldiğini garantiler. Herhangi birinin yerine yasal olmayan şekilde mesaj gönderilmesini engeller. Gizlilik, mesajların içeriğinin başkaları tarafından okunamamasını garantiler. Hattı dinleyenlerin kimlerin iletişim kurduğunu tespit edememesi trafik çözümleyici koruma ile sağlanır. ESP (Kılıflama Güvenlik Protokolü) başlığı mesajın değişimine karşı koruma sağlarken, veri gizliliğini de sağlamaktadır. Bunun yanısıra Kimlik Doğrulama başlığı, gizlilik sağlamadan mesajın içeriğinin değiştirilmesine karşı koruma sağlar. [27]

- Biyometrik Cihazlar: Biyometri, kişileri biyolojik özellikleri aracılığıyla tanımlamaktır. Güvenlik ihtiyaçlarının artması ve güvenliğin şifrelerle

karşılanmasındaki yetersizliklerden dolayı biyometrik sistemlerin geliştirilmesi kaçınılmaz olmuştur.

Günümüzde kullanılan biyometrik tanıma sistemleri; yüz tanıma, parmak izi tanıma, imza tanıma, kulak tanıma, retina ve iris tanıma olarak belirtilebilir. [5]

Yüksek güvenlik gereken yerlerde biyometrik cihazlar kablosuz akıllı kartlara, dizüstü bilgisayarlara entegre edilerek kullanılabilir. Ayrıca, biyometrik cihazlar kimlik doğrulama ve veri gizliliği için VPN çözümlerinde kullanılabilir.

6. SONUÇ

Kablosuz yerel alan ağları, hayatımıza sağladığı kolaylıklar ve esneklik dolayısıyla son yıllarda hayatımıza çok hızlı bir şekilde girmektedir. Ancak sağladığı avantajların yanısıra güvenlik ile ilgili açıklarının bulunması ve bu açıklara önlem olarak her geçen gün yeni ve farklı teknolojilerin geliştirildiği görülmektedir. Dolayısıyla bu sistemi kullanmak isteyen her türlü organizasyonun güvenlik tehditlerini ve unsurlarını göz önünde bulundurarak doğru bir WLAN sistem planlaması yapması gerekmektedir.

802.11 WLAN standardında belirtilen güvenlik açıklarını ortadan kaldırmak adına IETF (Internet Engineering Task Force-) ve IEEE tarafından çalışmalar yapılmış ve geliştirme çalışmaları devam etmektedir. IEEE, WLAN güvenliği artırabilmek için üç ayrı adımda çalışmalarını yürütmüştür. Bunlardan birincisi, 802.1i Çalışma Grubu'dur. Bu çalışma grubu, Gelişmiş Şifreleme Standardına (AES) dayalı şifrelemeyi desteklemektedir. AES tabanlı çözüm, WEP'e göre daha güvenli ve güçlü bir yapı sunmaktadır. Bu çözüm WEP'in güvenlik açıklarını kapatmak için geliştirilmiştir.

WLAN güvenliğini artırmak için ikinci adım, i çalışma gurubunun geçici çözümü olan WPA' dır. Bu protokol de WEP protokolünün açıklarını kapatmak amacıyla kullanılmıştır. TKIP protokolünü tanımlayan bu çalışma gurubu herhangi bir donanımsal değişime gerek kalmadan problemleri çözmektedir. WPA, zayıf RC4 algoritması yerine TKIP algoritmasını da kullanabilmekte ve böylece şifreleme daha güvenli hale getirilmektedir. WPA, WEP'in kullandığı 40 bitlik anahtar yerine 128 bit anahtarı kullanmakta olduğundan daha güçlü bir yapıya sahiptir. Aynı şekilde başlangıç vektörlerine bakıldığında, WEP protokolündeki başlangıç vektörünün tekrarlarından kaynaklanan güvenlik risklerine karşılık, WPA'da 48 bit kullanılmaktadır. Dolayısıyla başlangıç vektörünün tekrarlanma olasılığı azalmaktadır. WEP protolünde herhangi bir anahtar yönetimi kullanılmamasına rağmen, WPA protokolünde anahtar yönetimi her paket için 802.1X ile yapılmaktadır. Ayrıca WEP protokünde anahtar değişimi söz konusu değildir. Veri

bütünlüğüne bakıldığında WEP, Bütünlük Kontrol Değeri (ICV) kullanırken, WPA protokolünde Mesaj Bütünlük Kontrol protokolü (MIC) kullanılmaktadır. Asıllama yöntemi olarak WEP protokolünde tek taraflı bir yöntem kullanılırken, WPA'da 802.1x/EAP ile karşılıklı kimlik asıllama yöntemi kullanılmaktadır.

Bir diğer adım ise port tabanlı ağ erişim kontrolünü ve anahtar dağıtımı sağlayan, 802.1X standardının kullanımıdır. EAP protokolünün kullanımı ile, 802.1X erişim noktası ile kablosuz istasyonun birbirlerini karşılıklı asıllaması sağlanmış olur. WPA protokolünden sonra 802.11i standardına dayalı olarak geliştirilen WPA2 protokolü asıllama ve anahtar yönetiminde 802.1X kullandığından dolayı WEP'e göre daha güvenlidir. Şifreleme yöntemi olarak Gelişmiş Şifreleme Standardı AES kullanmaktadır.

Tüm bu geliştirilen standartlara rağmen güvenlik konusunda yönetimsel, operasyonel ve teknik olarak alınabilecek önlemler göz önünde bulundurulmalıdır. Maliyeti yüksek olmasına rağmen güvenliğin yüksek olması gereken kritik bilgilerin olduğu ağlarda kablosuz ağ uygulaması için donanımsal çözümlerden PKI uygulamaları, akıllı kartlar, biyometrik cihazlar, kablosuz ağlar için geliştirilmiş saldırı algılama sistemi IDS kullanılmalıdır.

KAYNAKLAR

1. Vines R. D., "Wireless Security Essentials: Defending Mobile Systems from Data Piracy", Wiley, Canada, 2002
2. Earle A.E., "Wireless Security Handbook", Auerbach Publications, US, 2006
3. Sankar k., Sundaralingam S., Miller D., Balinsky A., "Cisco Wireless LAN Security (Networking Technology)", Cisco Press, 2004, USA
4. Furht B., İlyas M., "Wireless Internet Handbook: Technologies, Standards, and Applications", Auerbach Publications, ISBN-10: 0849315026, 2003
5. **Dubendorf V. A., Wireless Data Technologies Reference Handbook,** Wiley, 2003, England
6. Seyman, M.N., Dikgen Frekans Bölüşümlü Çogullama Sistemlerinde Senkronizasyon Teknikleri, Yüksek Lisans Tezi, Erciyes Üniversitesi, Kayseri, 2005
7. Morelli M., Timing and Frequency Synchronization for the Uplink of an OFDMA Systems, IEEE Transactions on Communications, 52(2), 296-306
8. Ohrtman F., Roeder K., "Wi-Fi Handbook : Building 802.11b Wireless Networks", McGraw-Hill Professional Publications, USA, 2003
9. http://www.tutorial-reports.com/wireless/wlanwifi/introduction_wifi.php, Kasım 2006
10. http://www.tutorial-reports.com/wireless/wlanwifi/wifi_architecture.php, Kasım 2006
11. http://www.tutorial-reports.com/wireless/wlanwifi/wifi_datalink_layer.php, Kasım 206
12. http://www.tutorial-reports.com/wireless/wlanwifi/standards.php, Kasım 2006
13. "A Comprehensive Review of 802.11 Wireless LAN Security and the Cisce Wireless Security Suite White Paper", Cisco Systems, 2002
14. Internet Security Systems, " Wireless LAN Security, 802.11b and Corparete Networks, An ISS Technical White Paper", Atlanta, 2005
15. http://www.microsoft.com/technet/network/wifi/wifisoho.mspx, Mart 2007
16. Huang J., Susilo W., Seberry J., " Observations on the Message Integrity Code in IEEE802.11Wireless LANs", University of Wollongong, 2004, http://ro.uow.edu.au/cgi/viewcontent.cgi?article=1514&context=infopapers, Mayıs 2007
17. Geier J., "WPA Security Enhancements", March 20, 2003, http://www.wi-fiplanet.com/tutorials/article.php/2148721, Mart 2007
18. http://standards.ieee.org/getieee802/download/802.11i-2004.pdf, Aralık 2006

19. Örencik B. “Bilgisayar Ağlarında Güvenlik, Telsiz Ağ Güvenliği”, www3.itu.edu.tr/~orencik/TelsizAglardaGuvenlik.doc
20. Karygiannis T., Owens, “Wireless Network Security, 802.11, Bluetooth and Handheld Devices”, NIST Special Publication800-48, Gaithersburg, 2002
21. Tuğral N. “Kablosuz Bilgisayar Ağlarının Karşılaştırılmalı İncelenmesi, Yüksek Lisans Tezi”, Ankara, 2006
22. http://en.wikipedia.org/wiki/Direct-sequence_spread_spectrum, Kasım 2006
23. http://www.cisco.com/en/US/products/hw/wireless/ps430/products_white_paper09186a00800b469f.shtml, Aralık 2006
24. http://www.kirbas.com/index.php?id=267, Nisan 2007
25. http://www.windowsecurity.com/articles/Virtual_Private_Networking.html, Mayıs 2007
26. http://www.au-kbc.org/bpmain1/PKI/PKIieee.pdf, Nisan 2007
27. http://cisn.odtu.edu.tr/2003-9/pki.php, Nisan 2007
28. http://technet2.microsoft.com/WindowsServer/tr/Library/e9ee44d6-4ac8-4626-8012-7b46a4258c051055.mspx?mfr=true, Mayıs 2007
29. http://www.pcsupportadvisor.com/nasample/t1523.pdf, Kasım 2006
30. http://www.nig.abel.co.uk/network_intrusion_detection_systems.htm#2.2, Mayıs 2007

ÖZGEÇMİŞ

Fatma ULUCAN, 27 Eylül 1976 yılında İzmir'de doğdu. Lise öğrenimini İzmir Çınarlı Teknik Lisesi'nde tamamladıktan sonra 1995 yılında Marmara Üniversitesi Elektronik ve Bilgisayar Eğitimi Bölümü'nü kazandı. Bu bölümden 2000 yılında mezun oldu. 2001 yılı Eylül ayında Ted İstanbul Koleji'nde Bilgisayar Öğretmeni olarak çalışmaya başladı. 2004 yılında Maltepe Üniversitesi Fen Bilimleri Enstitüsü'nde Bilgisayar Mühendisliği Anabilim Dalı'nda yüksek lisans çalışmalarına başladı. 2007 yılında yüksek lisansı başarıyla tamamladı. **Fatma ULUCAN,** 2003 yılından beri Bilgisayar Zümre Başkanı olarak Ted İstanbul Koleji'nde görevine devam etmektedir.