İSTANBUL ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

KABLOSUZ GÜVENLİK PROTOKOLLERİNİN KARŞILAŞTIRMALI ANALİZİ

Bilgisayar Müh. Gülsüm Zeynep GÜRKAŞ
Bilgisayar Mühendisliği Anabilim Dalı

Danışman
Doç. Dr. A. Halim ZAİM

Temmuz, 2005

İSTANBUL

ÖNSÖZ

Bu çalışma İstanbul Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalında yapılan "Kablosuz Güvenlik Protokollerinin Karşılaştırmalı Analizi" adlı yüksek lisans tez çalışmasını içermektedir.

Bu tez çalışması boyunca gösterdiği her türlü destek ve yardımdan dolayı çok değerli hocam Sayın Doç.Dr.A.Halim ZAİM'e, bu çalışmanın yürütülmesinde bilgisini ve manevi desteğini esirgemeyen çok değerli çalışma arkadaşım Araş.Gör.M.Ali AYDIN'a en içten dileklerimle teşekkür ediyorum.

Ayrıca tüm eğitim hayatım boyunca bana yol gösteren, destek olan, en önemlisi bana eğitimin ne kadar önemli olduğu bilincini ve çalışma disiplinimi kazandıran , her zaman yanımda olan aileme en içten dileklerimle teşekkürlerimi sunuyorum.

Gülsüm Zeynep GÜRKAŞ
Temmuz 2005

İÇİNDEKİLER

ŞEKİL LİSTESİ

TABLO LİSTESİ

KISALTMALAR

WLAN : Wireless Local Area Networks
RF : Radio Frequency
Wi-Fi : Wireless Fidelity
IEEE : Institute of Electrical and Electronics Engineers
PHY : Physical Layer
MAC : Medium Access Control
LLC : Logical Link Control
DCF : Distributed Coordination Function
PCF : Point Coordination Function
FHSS : Frequency Hopping Spread Spectrum
DSSS : Direct Sequence Spread Spectrum
BSS : Basic Service Set
IBSS : Independent BSS
STA : Station
AP : Access Point
SSID : Service Set Identifier
OFDM : Orthogonal Frequency Division Multiplexing
IR : Infrared
CSMA/CA : Carrier Sense Multiple Access with Collision avoidance
NIC : Network Interface Card
RTS : Request to Send
CTS : Clear to Send
WEP : Wired Equivalent Privacy
WPA : Wi-Fi Protected Access
TGi : IEEE Task Group "i"
FMS : Fluhrer-Mantin-Shamir
ICV : Integrity Check Value
IV : Initialization Vector
RC4 : Rivest Cipher 4
CRC : Cyclic Redundancy Check
TKIP : Temporal Key Integrity Protocol
MIC : Message Integrity Code
AES : Advanced Encryption Standart
EAP : Extensible Authentication Protocol
CBC-CCMP : Counter Mode Cipher Block Chaining Message Authentication Code Protocol

ÖZET

KABLOSUZ GÜVENLİK PROTOKOLLERİNİN KARŞILAŞTIRMALI ANALİZİ

Kablosuz Yerel Alan Ağları günümüzde hızla büyümekte ve özellikle iş dünyasında ve bilgisayar sektöründe popülerliği artmaktadır. Popülerlikle beraber artan üretkenlik hem fiziksel katmanda hem de güvenlik mekanizmalarında birçok gelişmeye neden olmuştur.

Kablosuz Yerel Alan Ağları (Kablosuz LAN) için kullanılan standartlar IEEE tarafından geliştirilen 802.11 ailesidir. Bu standartların gelişimi 1997 yılında 802.11 ile başlamıştır. 1999 yılında 802.11b ve 802.11a, 2003 yılında da 802.11g standart haline gelmiştir. 802.11i ise var olan 802.11 standartları üzerinde güvenlik iyileştirmelerini içermektedir.

Kablosuz LAN sistemlerinde ilk nesil güvenlik protokolü WEP'tir. Şifreleme algoritması olarak RSA Data Security tarafından geliştirilen RC4 algoritmasını kullanır. WEP'in birçok güvenlik açığı tespit edilmiştir. Bu güvenlik açıklarını gidermek için ikinci nesil güvenlik protokolü 802.11i geliştirilmeye başlanmıştır fakat kısa vadede bir ara çözüm sağlayabilmek için Wi-Fi Protected Access adlı sistem ortaya çıkmıştır. WPA'da TKIP protokolü WEP'e bir güncelleme olarak tasarlanmıştır. 802.11i WEP ve TKIP'ın yerini alması için CBC-CCMP protokolünü tanımlamaktadır. Bu sistem şifreleme algoritması olarak AES'i kullanır.

Bu çalışmada kablosuz LAN sistemlerinin performansı incelenmiştir. Çalışmanın birinci kısmında 802.11b, 802.1g ve 802.11i standartlarının fiziksel katmanı desteklediği farklı veri hızlarını da içerecek şekilde gerçeklenmiştir. Bu kısımda günümüzde kablosuz LAN'lar için var olan güvenlik mekanizmalarının sistem performansına olan etkisinin incelenmesi hedeflenmektedir. Bu amaçla uygun güvenlik mekanizmaları gerçeklenmiştir. Ele alınan mekanizmalar iki farklı anahtar uzunluğu (40 bit ve 104 bit) ile WEP, WPA ve WPA2'dir. Bu mekanizmaların ağ performansı üzerindeki etkileri değerlendirilerek, güvenlik düzeyinin ve karmaşıklığının artışının performansı düşürdüğünün görülmesi hedeflenmiştir.

Çalışmanın ikinci kısmında ise 802.11g ağların performansı birden çok istemci ve bir erişim noktası ile kurduğumuz bir ağ üzerinde inceleyen deneysel çalışmalar yapılmış, ağ trafiği ve belirlediğimiz güvenlik katmanlarının uygulaması yapılmıştır. Bu deneysel çalışmanın sonucu ile doğrulama ve şifreleme sistemlerini barındıran bu katmanlı yapının performans üzerindeki etkisinin görülmesi hedeflenmiştir.

SUMMARY

A COMPARATIVE ANALYSIS OF WIRELESS SECURITY PROTOCOLS

Wireless Local Area Networks are rapidly growing. They also continue to gain popularity, especially in businness and computer industry. The increased productivity and growing popularity caused many improvements on both physical layer and security mechanisms.

The communication standarts for wireless LANs are 802.11 family designed by IEEE. The development of these standarts started with 802.11 in 1997. The following standarts are 802.11a ve 802.11b in 1999 and 802.11g in 2003.Today the most popular standart in wireless LANs is still 802.11b. The latest standart 802.11i,designed in 2004, includes security improvements on existing 802.11 standarts.

The first generation security mechanism of WLANs is WEP . It employs RC4 algorithm from RSA Data Security. WEP has lots of security flaws. The second generation security mechanism to provide more reliable communication is 802.11i but an intermediate solution solution called WPA has been developed as a short term solution. TKIP has been designed as a patch for WEP in WPA. 802.11i specifies CBC-CCMP to supersede WEP and TKIP. It employs AES as encryption algorithm and also called WPA2.

In this study we investigated the performance of wireless LANs. In the first part of our study we impelemented the physical layer of 802.11b, 802.11g and 802.11i with appropriate and different data rates. We measured the performance of the network structure without using any security mechanisms. The performance measurements of our simulation study are total communication time and throughput. Then we implemented the security mechanisms available for wireless LANs today. We investigated the impacts of the security mechanisms on the performance of networks. The security mechanisms that we implemented are WEP with two different key lengths (40 bits and 104 bits), WPA and WPA2. The impact of the these security mechanisms on network performance has been obtained in order to see that as the complexity of security mechanism increases the network performance decreases.

In the second part of our study we investigated the performance of a real 802.11g network with two computers and an access point with our experimental studies. We have generated network traffic on this network and applied the security levels we have decided. We obtained the results and statistics in order to see the effects of network encyption and authentication mechanisms in these security levels.

.

1.GİRİŞ

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

Kablosuz ağların artan uygunluğu ve bağlı olarak kablosuz ağlara olan güvenin artmasıyla, ağda meydana gelebilecek başarısızlıklara veya güvenlik açıklarına rağmen, güvenilir ve sağlam iletişim gerçekleştirebilmek oldukça önem kazanmaktadır.

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

Bu tez çalışmasında IEEE 802.11 WLAN sistemleri için günümüze kadar geliştirilmiş güvenlik mekanizmaları ele alınmıştır. Bu mekanizmaları barındıran "güvenli" ağların performansı konusu üzerinde durulmuştur.

Bölüm 2'de öncelikle kablosuz yerel alan ağlarının tanımı yapılarak avantaj ve dezavantajları incelenmiş, IEEE 802.11 Standartları ve mimarisi ve 802.11 ağlarında günümüze kadar gelişmiş güvenlik mekanizmaları anlatılmıştır.

Bölüm 3'te 802.11 ağların güvenliği için geliştirilen sistemler ve bu sistemlerde kullanılan algoritmalar ayrıntılı bir şekilde anlatılmıştır. 802.11 WLAN sistemlerinin fiziksel özellikleri ve bu ağlar için geliştirilmiş olan güvenlik mekanizmalarının gerçekleştirilmesiyle geliştirilen simülasyonun ayrıntıları belirtilmiştir. Laboratuar ortamında kurulan küçük boyutlu bir 802.11g standardını destekleyen gerçek ağ üzerinde deneysel çalışmanın ayrıntılarına yer verilmiştir.

Bölüm 4'te ilk olarak 802.11b, 802.11g ve 802.11i ağlar ve güvenlik mekanizmaları simülasyon yardımıyla incelenmiştir. Sistem performansının değerlendirilebilmesi için yararlı yük (throughput) ve toplam süre göz önüne alınmıştır. İkinci bölümde anlatılan deneysel çalışmanın sonuçları ise özel bir yazılım kullanılarak toplanmış ve yorumlanmıştır.

Bölüm 5'te öncelikle güvenlik mekanizmalarının sistem performansı üzerindeki etkileri incelenmiştir. Akabinde farklı güvenlik mekanizmalarının karmaşıklığı ve ağ topolojisi ile sistem performansının etkileşimi ele alınmıştır. Deneysel çalışmanın sonuçları farklı başlıklar altında incelenmiştir.

2. GENEL KISIMLAR

2.1 KABLOSUZ YEREL ALAN AĞLARI

Kablosuz Yerel Alan Ağları (Wireless Local Area Networks, WLANs), iki yönlü geniş bant veri iletişimi sağlayan, iletim ortamı olarak kablo yerine radyo frekansı veya kızılötesi ışınları kullanan ve bina veya kampüs gibi sınırlı bir alanda çalışan iletişim ağlarıdır [1]. Kurulum kolaylığı ve hareket serbestliği gibi önemli avantajlar sağlayan WLAN sistemleri kablolu ağların yerini alabilmekte hatta bu ağlara göre daha fazla fonksiyonlar içerebilmektedir. Kablosuz Yerel Alan Ağları Avrupa düzenlemelerinde Telsiz Yerel Alan Ağları, Radio Local Area Networks, Radio LAN, RLAN olarak adlandırılmasına karşın başta ABD olmak üzere bir çok ülkede Wi-Fi (Wireless Fidelity – Kablosuz Bağlılık), Wireless Local Area Networks, Wireless LAN, WLAN olarak adlandırılmaktadır.

WLAN sistemleri iş adamları, yöneticiler, çalışanlar, küçük işletmeler, orta ölçekli işletmeler ve bireysel kullanıcılar gibi büyük bir kesime internet ve üyesi oldukları kurumsal ağa (Intranet) mobil olarak bağlanma imkanı sağlamaktadır. Ayrıca, WLAN sistemleri kullanıcılara mekandan bağımsız olarak kolay bir kablosuz ağ kurulumu ve geniş bant veri iletimi imkanı sunmaktadır [1, 3]. Kablolu LAN'ların tüm özelliklerine sahip olan WLAN sistemleri bu ağların devamı ya da alternatifi olarak kullanılmaktadırlar.

2.1.1. Kablosuz Ağların Avantajları

- *Esneklik:* Kablosuz iletişim radyo dalgaları aracılığı ile sağlandığı için kablosuz ağ araçları kullanan kişilerin sabit bir yere bağlı kalma zorunluluğu yoktur. Bu insanlara büyük bir ölçü de özgürlük sağlamakta ve verimliliği arttırmaktadır.
- *Kolay Kurulum:* Kolay kurulumu da kendi içinde iki faydası vardır:
    - Zaman: Radyo dalgaları ile iletişim yapılmasından dolayı kablolu bir ağ tasarlanmasından önce gerekli olan kablolama planı ve kablolama işlemi için harcanan zamandan kazanılmış olunur.
    - Maliyet: Yukarıda belirtildiği gibi kablolama yapılmadığı için kablo maliyeti ağ kurulumunda yer almamaktadır.
- *Sağlamlık:* Kablolu ağlarda kablolara gelebilecek zararlardan ağ yapısı ciddi şekilde etkilenebilir. Örneğin bir felakette kablolar kopabilir ya da dış etmenlerden kullanılmaz hale gelebilir. Fakat telsiz yapılarda bu tip problemlerle karşılaşılmaz.

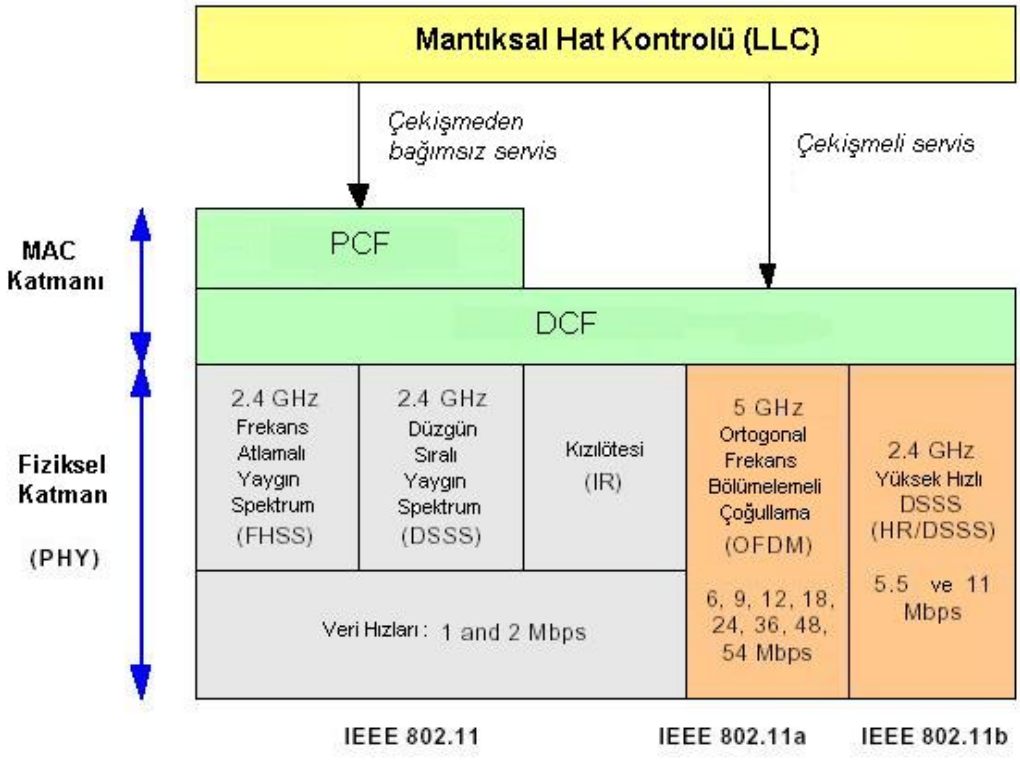
2.1.2. Kablosuz Ağların Dezavantajları

- *Güvenlik:* Yapılan iletişim dalgalar halinde yayıldığı için arayan giren bir kişinin dinlemesi ve verileri ele geçirmesi kablolu yapıya göre daha kolaydır.
- *İletişim Hızı:* Çeşitli faktörlerden dolayı iletişim hızı kablolu yapı kadar iyi değildir. Bu faktörlerin bazıları erişim noktasının yönünün değişmesi, araya engellerin girmesi, erişim noktasından uzaklaştıkça sinyalin zayıflaması olarak gösterilebilir.
- *Standartlara Uyma Zorunluluğu:* Üretilen cihazların tüm dünya standartlarında olması gerekmektedir. Uluslararası enstitüler bazı konularda sınırlamalar getirmekte ve bu da gelişmelerin daha yavaş olmasına neden olmaktadır. Örneğin kullanılabilecek frekanslar sınırlıdır ve istenilen frekansta haberleşme yapılamaz.[4]

2.2. IEEE 802.11 STANDARTLARI

IEEE (Institute of Electrical and Electronics Engineers) 802.11 standartını Ekim 1997 tarihinde onaylamış (IEEE 802.11b Standardı,1999) ve Mart 1999 tarihinde revize etmiştir. Bu standart yerel alan ağlarında kablosuz iletişimi sağlamak amacıyla üç farklı fiziksel (physical – PHY) katman ve bir ortam erişim kontrolü (medium access control – MAC) katmanı sağlar. Mantıksal Hat Kontrolü için (logical link control - LLC) 802 ailesine ait tüm standartlar için benzerdir.

MAC protokolü iki tip servise destek vermektedir. Bunlar dağıtık koordinasyon fonksiyonunu kullanan asenkron (distributed coordination function – DCF) ve noktasal koordinasyon fonksiyonu kullanan senkron (point coordination function - PCF) servislerdir.



Şekil 2.1 : 802.11 Protokol Yapısı

802.11 standartı temel olarak 1 ila 2 Mbps arasında frekans atlamalı yaygın spektrum (FHSS) veya düzgün sıralı yaygın spektrum (DSSS) kullanarak veri iletimi sağlayan spesifikasyonlar ailesidir. Daha sonra yapılan revizyonlar sonucunda 5 GHz frekans bantında ve 54 Mbps hızında işlem yapan 802.11a standartı ve ardından 2.4 GHz frekans bantında ve sırasıyla 11Mbps ve 54 Mbps hızlarında işlem yapan 802.11b ve 802.11g standartları geliştirilmiştir. Şekil 2.1'de 802.11 standartlarının protokol yapısı gösterilmektedir.

802.11 standardı son kullanıcı lisanslarına gerek duymaksızın birden çok kullanıcının radyo frekanslarının paylaşımına izin veren radyo spektrum teknolojilerinin avantajlarına da sahiptir. Ayrıca 802.11 ve 802.11b ağlar 2.4 GHz Industrial, Scientific and Medical (ISM) bandının ve 802.11a temelli ağlar da Unlicensed National Information Infrastructure (UNII) bandının kullanımını sağlamaktadır. International Telecommunication Union (ITU) ise her ikisini de tanımlar. Ancak enterferans (karışma) konusu özellikle 2.4 GHz bandında hala bir sorun teşkil etmektedir. Eğer havayolları radyo frekansı gibi resmi ve yetkili bir kullanıcı ile çarpışma yaşanırsa operasyon duracaktır. Ayrıca, 802.11 frekanslarına erişebilen Bluetooth gibi teknolojilere karşı hiçbir koruma mevcut değildir. [5]

2.2.1. Mimari

802.11 ağların (WLAN) mimarisi temel olarak birbirini kısmen kaplayabilen hücrelerden oluşur. Temel Servis Kümesi (Basic Service Set - BSS) tek bir hücrenin kapsama alanını temsil eder. Bir BSS'in dışında kalan bir istasyon (STA) bu BSS içinde kalan diğer istasyonlar ile haberleşemez.
802.11 standartları iki modda çalışmaktadır.Bunlardan ilki BSS olarak da bilinen altyapı modu diğeri ise Bağımsız BSS (Independent BSS- IBSS) olarak bilinen Bağımsız (Ad hoc) moddur.

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

En basit WLAN yapısı Bağımsız (ad hoc veya peer-to-peer) WLAN'dir. Bu WLAN NIC ile donanmış bir grup bilgisayarın kurdukları ağın ismidir. Bu tip konfigurasyona sahip bir ağda erişim noktasına ihtiyaç duyulmaz ve noktadan noktaya haberleşmeyi

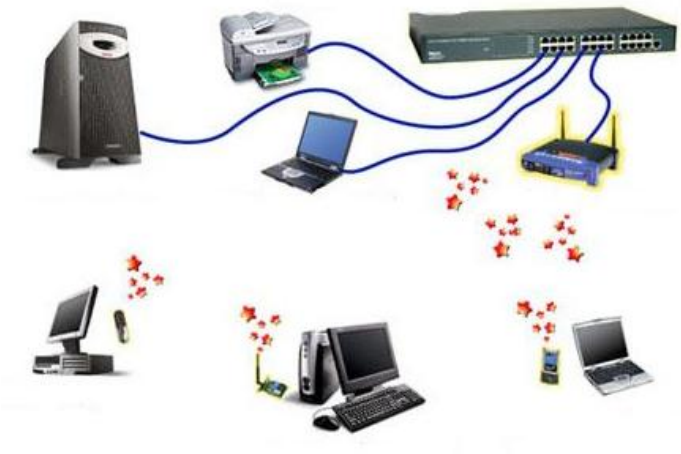
sağlamak amacıyla yerel ağ aynı radyo frekans kanalında çalışır. Birbirinden farklı ağlar ancak kablosuz adaptörler birbiriyle haberleşebilecekleri mesafedeyse oluşturulabilir.

Bu yapıda, her kullanıcı ağdaki bir diğeri ile direkt iletişim kurar. Bu mod, birbirleri ile iletişim mesafesinde olan kullanıcılar için tasarlanmıştır. Eğer bir kullanıcı bu tanımlanmış mesafeden dışarıya çıkarak iletişim kurmak isterse, aradaki bir kullanıcı, ağ geçidi ve yönlendirici olarak görev yapmak zorundadır. Şekil 2.2'de bağımsız WLAN mimarisinde ağ elemanlarının yerleşimi görülmektedir.

Şekil 2.2 : Bağımsız (Ad Hoc) WLAN Mimarisi

2.2.1.2. Altyapı Modeli (Infrastructure Mode)

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

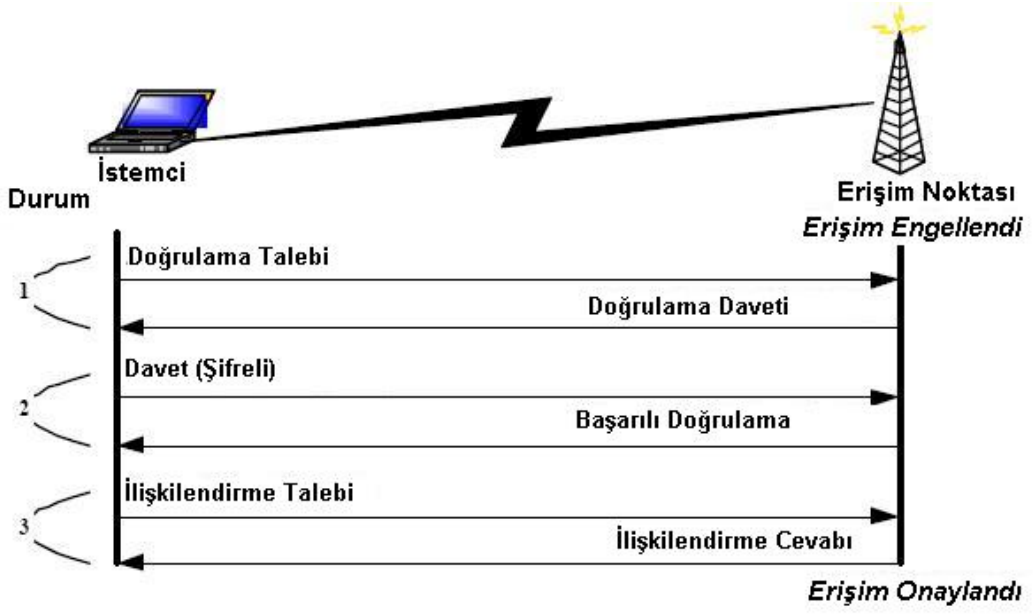


Şekil 2.3 : Altyapı Moda WLAN Mimarisi

Şekil 2.3'te tek AP içeren ve altyapı modunda çalışan bir ağın genel yapısı görülebilir. Bir AP tarafından koordine edilen alana BBS (Basic Service Set) ismi verilmektedir. Bunun anlamı 'bir tek koordine merkezi tarafından idare edilen bir grup istasyondur'. Geniş ağlarda AP'ler de birbirine kablolu ağlar yardımı ile bağlanmaktadır. Kablolu ağlarda bir ağı tanımlamak için Ağ Adresi (Network Address) kullanılmaktadır. Kablosuz ağlarda ise ağı tanımlamak için ise SSID (Service Set Identifier) kullanılmaktadır. Kullanımı ise şu şekildedir: Bilgisayarda yüklü yazılım yardımı ile bağlanılabilecek SSID numaraları belirlenir ve bunlardan biri seçilerek ilgili ağa bağlantı yapılır. Tabii ki bilgisayarların bu SSID numaralarına erişebilmeleri için AP'lerin bu numaraları çeşitli aralıklarla yaymaları (broadcast) gerekmektedir. Aynı alan içerisinde farklı komünikasyon kanallarını kullanan (Örneğin, frekans bölümlemeli çoğullma yöntemi) ağlar mevcut olabilmektedir.

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

a) Doğrulanmamış ve ilişkilendirilmemiş : Kullanıcının ağ ile doğrulama ve ilişkilendirme işlemlerini gerçekleştirmediği durumdur.
b) Doğrulanmış ve ilişkilendirilmemiş : Kullanıcının ağ ile doğrulama işlemi gerçekleştirdiği fakat henüz ilişkilendirme işlemini gerçekleştirmediği durumdur.
c) Doğrulanmış ve ilişkilendirilmiş : Kullanıcının ağ ile doğrulama ve ilişkilendirme işlemlerini tamamlandığı durumdur.



Şekil 2.4 : Doğrulama ve İlişkilendirme Durumları

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

2.2.2. Mikrohücreler ve Gezginlik

Bir erişim noktasının kapsama alanına "microcell' denir. Çoklu erişim noktalarının gerektiği bölgelerde kullanıcıların herhangi bir yerde hatdışı kalmalarını ve erişim noktaları arasında yeniden giriş yapıp uygulamalarını yeniden başlatmalarını engellemek çok önemlidir. Ancak erişim noktalarının kullanıcı bağlantısını birbirleri arasında hand off (el verme) sistemiyle aktarabilmelerinden geçer. Overlap (birbiri üzerine geçme) durumlarında kablosuz araçlar ve erişim noktaları sık sık iletimin kalitesini ve gücünü ölçmelidirler. WLAN sistemi o an için en güçlü ve en iyi kalitedeki sinyali veren erişim noktasından hizmet vermeye yönelik olmalıdır ve kullanıcı bu gezginlik işlemini bir an için bile hissetmemelidir. [6-8]

2.2.2. Fiziksel Katmanlar

Fiziksel katman verinin radyo sinyalleri ve hava ortamı arasındaki işleme sürecini gerçekleştirmektedir. 802.11 standartları beş farklı fiziksel katman tanımlamaktadır.[5] Bunlar ;

- Frekans Atlamalı Yaygın Spektrum (FHSS)
- Düzgün Sıralı Yaygın Spektrum (DSSS)
- Yüksek Hızlı Düzgün Sıralı Yaygın Spektrum (HR/DSSS)
- Ortogonal Frekans Bölümlemeli Çoğullama (OFDM)
- Kızılötesi (IR)

Bunlardan ilk üç fiziksel katman radyo yaygın spektrum teknolojisidir ve 2.4 GHz bandında çalışırken, OFDM 5 GHz bandında çalışır. IR ise 300 – 428 Hz bandında düşük hızla ve görüş alanında bulunma koşuluna bağlı olarak kurulan bir bağlantı ile çalışır.

2.2.2.1 FHSS

FHSS geniş bir frekans aralığında, veri sinyallerini bir frekanstan diğerine atlayan taşıyıcı bir sinyal ile modüle eder. Ölçü olarak zaman kullanılır. Çarpışmaları önlemek amacıyla taşıyıcı frekansı 2.4 ve 2.438 GHz arasında periyodik olarak değişir. Bir çarpışma ancak ve ancak bir dar bant sistemin ve yaygın spektrum sinyallerinin aynı frekansta ardı ardına iletim yapması durumunda meydana gelir. Hangi frekansa atlanacağının kararı ve veri iletimin sırasını belirlemek amacıyla bir atlama kodu (hopping code) kullanılır. FHSS maksimum 2 Mbps hızında bir iletim sağlar.

2.2.2.2 DSSS ve HR/DSSS

DSSS gönderim yapan istasyondaki veri sinyalini Chipping kodu veya işlem kazancı olarak bilinen daha yüksek veri hızına sahip bir bit dizisiyle birleştirir. Bu kod yayılma oranlarına bağlı olarak kullanıcı verisini bölerek engel ve karışmaları azaltır ve 11 Mbps hızında veri transferini mümkün hale getirir. Her veri biti için yollanmak üzere özel bir bit katarı belirlenir ve chipping koda karışmalara karşı dayanıklılığı arttırmak amacıyla fazladan bir bit örneği de eklenir.

2.2.2.3 OFDM

OFDM, 802.11a standardında daha az karışma sağlamak amacıyla yaygın spektrum teknolojileri yerine kullanılmaktadır. Bu metot 54 Mbps hızında yüksek hızlı veri iletimi sağlar. OFDM yöntemi radyo sinyallerini farklı frekanslarda (çoklu taşıma) aynı anda yollanmak üzere daha kısa sinyallere böler ve böylece iletim boyunca oluşabilecek çapraz karışmaları (croosstalk-elektronik çarpışma) önlemeyi hedefler.

2.2.3. MAC Katmanı

802.11 spesifikasyonları asenkron (Distribution coordination function - DCF) ve çekişmeden-bağımsız (Point coordination function - PCF) servisler sağlamaktadır. Çekişmeden bağımsız servis isteğe bağlıyken asenkron servis her zaman erişilebilir durumdadır. DCF ortam paylaşımı için 802.11 MAC protokolünün temel erişim metodu olan çarpışma sakınmalı taşıyıcı dinleyen çoklu erişim (carrier senses multiple access with collision avoidance-CSMA/CA) tekniğini kullanır. PCF ise sorgulamalı (polling) erişim metodu ile çekişmeden bağımsız bir servis sağlar. Genellikle AP nokta koordinatörü (point coordinatator -PC) olarak görev yapar ve periyodik olarak tüm istasyonları sorgular ve onlara iletim yapma imkanını tanır. Bu yüzden PCF tarafından sağlanan erişim önceliğinden, çekişmeden bağımsız bir erişim mekanizması yaratmak için yararlanılır. PC istasyonların çerçeve iletimlerini sınırlı bir zaman periyodunda çekişmeleri elemek için kontrol eder. DCF'nin tersine PCF'nin uygulanması zorunlu değildir. Ayrıca PCF'nin kendisi DCF tarafından sağlanan asenkron servise dayanmaktadır. Tüm fiziksel katmanlar ortak bir MAC katmanını desteklemektedir. 802.11e çalışma grubu QoS için MAC katmanının iyileştirilmesi ile ilgili çalışmaktadır.

2.2.4. Fiziksel Elemanlar

802.11 ağlar beş ana fiziksel elemandan oluşur. Bunlar Dağıtım Sistemi (Distribution System), Erişim Noktası (Access Point), Kablosuz Ortam (Wireless Medium) ve İstasyonlar (Stations) ile Ağ arayüz Kartları (Network Interface Cards) olarak adlandırılır. [7,9]

2.2.4.1. Dağıtım sistemi (DS)

Birden fazla temel servis kümesi (BSS) ve yerel alan ağlarını (LAN) entegre ederek Genişletilmiş Servis Kümesi (ESS) oluşturan sisteme verilen addır.

2.2.4.2. Erişim Noktaları (AP)

Kablosuz ortama bağlanmış olan istasyonların dağıtım sistemine erişimini sağlayan ve aynı zamanda bir istasyon özelliğine de sahip olan ağ elemanıdır.

Access Point (AP) kablolu ağlardaki LAN hub cihazı ile aynı işlemleri yapar. Yaptığı iş kablolu altyapıya sahip ağlara standart bir Ethernet kartıyla bağlanmak ve tıpkı bir anten gibi kablosuz araçların birbiriyle haberleşmesini sağlamaktır. AP belirli bir frekans bandında çalışır ve 802.11 de belirtilen modülasyon tekniklerini kullanır.

2.2.4.3. Kablosuz Ortam

Kablosuz yerel alan ağlarında fiziksel katman bileşenleri arasında protokol veri birimlerinin (PDU) transferi için kullanılan ortamdır.

2.2.4.4. İstasyonlar

Kablosuz ortama erişebilmek için gerekli olan fiziksel katman arayüzüne ve uygun 802.11 ortam erişim kontrolüne (medium access control - MAC) sahip olan cihazdır.

2.2.4.5. Ağ Arayüz Kartı /İstemci Adaptörü

Kablosuz İstemci adaptörleri PC veya iş istasyonlarını kablosuz bir network'e bağımsız modda ya da altyapı modunda olmak üzere erişim noktaları yardımıyla bağlar. PCMCIA (Personal Computer Memory Card International Association) kartı ve PCI (Peripheral Component Interconnect) ile masaüstü ve mobil hesaplama cihazları bütün ağ kaynaklarına kablosuz olarak erişebilir.

NIC, bağlantı için uygun olan frekans spektrumunu tarar ve bir erişim noktası veya başka bir kablosuz istemci ile iletişime geçer. NIC PC/Workstation işletim sistemlerine sürücü yazılım güncellemesi olarak eklenebilir.

2.2.5. Standartlar

2.2.5.1. 802.11

IEEE 802.11, ilk kablosuz yerel ağ standardıdır [10]. Bu standart 2.4GHz bandında çalışır ve farklı işlem şekillerini destekler. Veri transferi için Barker kodlama tekniği kullanılarak 2 Mbps hızına kadar veri iletimi sağlar. Her gün gelişen teknolojiye paralel olarak, bu standarda ilişkin veri oranları ve etkili modulasyon teknikleri geliştirilmektedir.

2.2.5.2. 802.11a

802.11a standardı 1999 yılında kablosuz asenkron transfer modu (ATM) için geliştirilmiştir ve 5 GHz frekans bandında işlem yapan Ortogonal Frekans Bölümlemeli Çoğullama (Orthogonal Frequency Division Multiplexing - OFDM) kullanır [11]. Bu standart ile 54 Mbps hızına kadar yüksek veri iletim oranı sağlanmaktadır. Buna rağmen, bu standart 5 GHz Unlicensed National Information Infrastructure (U-NII) bandını kullanır. Veri oranları sinyallerin sönümleme (fading) ve çoklu yol (multipath) yansımalar nedeniyle çok kısa mesafeyle sınırlandırılmaktadır.

2.2.5.3. 802.11b

802.11b 1999 yılında geliştirilmiştir ve aynı zamanda Yüksek Hızlı 802.11 veya Wi- Fi olarak da bilinir.[12] Bu standart 2 GHz Industrial-Scientific- Medical (ISM) frekans bandında işlem yapan Tümleyici Kod Anahtarlama (Complementary Code Keying - CCK) modulasyonunu ve HR/DSSS tekniğini kullanmaktadır. Bu standart ile 11Mbps hızına kadar yüksek veri iletim hızı desteklenmektedir ve çoklu yol yayılma çarpışmalarına karşı daha dayanıklıdır. Bu standart ayrıca 11 Mbps'dan 33Mbps'a kadar ulaşan veri iletim oranlarını destekleyebilen PBCC (Packet Binary Convolutional Coding) seçeneğini de içermektedir. 802.11 standardı ile geriye yönelik olarak uyumludur. Mikrodalga fırınlar, kablosuz telefonlar ve Bluetooth gibi diğer kablosuz teknolojilerle olan çarpışma olasılığı ise getirdiği kısıtlamalardan biridir. [5]

2.2.5.4. 802.11g

802.11'in içerdiği iki standarttan biri olan 802.11b'nin tasarlanması ve inşası çok basittir. 802.11a ise karmaşık bir yapıya sahiptir. 802.11a'nın tasarımı bittikten sonra bile pazardaki yerini alırken birkaç zorlukla karşılaşılmıştır. Bunlar 802.11b'nin birçok kullanıcı tarafında kullanılması, iki standardın birbiri ile uyumlu olmaması ve 802.11a'nın sadece kısa mesafelerde erişebilirlik sağlamasıdır.

IEEE uzun mesafelerde de yüksek veri iletim hızını gerçekleştirebilme düşüncesiyle bir takım oluşturmuştur ve bu iki standardın da kendine ait iyi özellikleri alınarak bir hibrid (karma) standart geliştirilmiştir. Bu standart IEEE tarafından 802.11g olarak isimlendirilmiştir. 802.11g standardı, 802.11a standardından gelen teknolojiye uyumlu olup, 2.4 GHz frekans bandında işlem yapan 802.11b ile birlikte uyumluluk sağlar. 802.11g tarafından kullanılan OFDM teknolojisi 802.11a standardına uyumludur. OFDM 6, 9, 12, 18, 24, 36, 48 ve 54 Mbps veri hızlarını sağlar. 802.11a ise sadece kısa mesafelerde 5 GHz frekans bandında çalışarak aynı teknolojiyi kullanır. 802.11g 802.11b ile benzer şekilde 2.4 GHz frekans bandında işlem yapar. 802.11b 1, 2, 5.5 ve 11 Mbps veri hızlarını destekler ve veri iletimi için CCK kullanır.

802.11 standartlarınının fiziksel katman üzellikleri karşılaştırmalı olarak Tablo 2.1'te özetlenmiştir.

Tablo 2.1 : 802.11 Standartlarının Fiziksel Katman Özelliklerinin Karşılaştırması

Fiziksel Katman	**Frekans**	**Modulasyon**	**Veri Hızları(Mbps)**	**Özellikler**
Wi-Fi (802.11b)	2.4 GHz	Barker Kodlama/ CCK	1, 2, 5.5, 11	-Yaygın WLAN Teknolojisi -Olgunlaşmış Teknoloji -Düşük Maliyet
802.11g	2.4 GHz	Barker Kodlama / CCK	1, 2, 5.5, 11	-54 Mbps'ye varan Hız - Yüksek Aralık -Wi-Fi ile geriye yönelik uyumlu
		OFDM	6, 12, 24, 36, 48, 54	
802.11a	5 GHz	OFDM	6, 12, 24, 36, 48, 54	-54 Mbps'ye varan Hız - Yüksek seviye ölçeklenebilirlik

2.2.5.5. İletimin Fiziksel Özellikleri

İletişim için kullanılacak modulasyon tekniği ne olursa olsun, tüm standartlar IEEE'nin WLAN'lar için oluşturduğu standartlardır. Aynı aileden gelen bu standartlar benzer paketleme yapılanmasına sahiptirler. 802.11 ailesinin paketlerinin hepsi bir başlama eki (preamble), başlık (header) ve bir yükten (payload) oluşmaktadır. Giriş kısmı ne kadar kısa olursa ağda dolaşımda o kadar fazla olacaktır. 802.11b, 120 μsec gibi uzun bir başlama eki kullanır, oysa 802.11g 96 μsec gibi kısa bir başlama eki kullanır. 802.11g cihazlari 3 tane üst üste binmemiş kanal kullanır ve Extended Rate Physical (ERP) katmanı olarak isimlendirilen yeni fiziksel katmana sahiptirler. 802.11g standardı tarafından veri iletimi sırasında çarpışma sakınma tekniği kullanılmaktadır. 802.11g'nin kullandığı CSMA / CA protokolü, veri göndericiye veri iletim kanalını kullanma hakkı gibi farklı özellikler sunar. İşlem gören bir veri iletimi sırasında mevcut iletim sonlandırılmadan başka hiçbir cihaz tarafından iletim yapılamaz. 802.11g standardı 802.11b standardı ile uyumlu olmasına rağmen, tek 802.11g ortamlarında veri oranlarını desteklemesiyle karşılaştırıldığında karışık ortamlarda yüksek veri oranlarını desteklemez.

2.5.5.6. Koruma Mekanizmaları

802.11g erişim noktalarındaki farklı konfigürasyonlar ve bir arada bulunan 802.11g ve 802.11b cihazları ağ yönetiminde birçok soruna sebep olmaktadır. Bundan sadece iletim hızları değil, aynı zamanda tüm ağın etkinliği ve tüm ağ üzerindeki cihazların işlem mekanizmaları da etkilenmektedir. Karışık bir ortamda, 802.11g standardını kullanan cihazlar veri iletimi için uzun başlama eki kullanmak zorundadırlar ve bu da ileri seviyeyi gerektirmektedir. Eğer uzun başlama ekleri kullanılmazsa, isteklerin sırasına bakılmaksızın paketlerden her zaman kısa olan başlama eklerinin düşünülerek alınma riski vardır. 802.11g ve 802.11b'nin bir arada olduğu karma ortamlarına tamamıyla uyum sağlamak için ekstra özelliklere sahip olabilmek gereklidir. Aksi takdirde OFDM sinyalleri hiçbir 802.11b cihazı tarafından alınamaz. Örneğin, 802.11g cihazı 802.11b cihazı tarafından algılanmayan bir CSMA/CA paketi gönderdiğinde, bu başka bir cihazın veri iletimi bitene kadar beklemesi gerekip gerekmediğini bilemediği için veriyi yollar ve sonuç olarak bir çakışma oluşur. Bu çelişkileri önlemek için, 802.11g standardı Request to Send (RTS)/ Clear to Send (CTS) gibi koruma mekanizmalarına sahip olmak zorundadır. Bu mekanizmalar, iletimde oluşacak her türlü çakışmayı

önlemekte yardımcı olurlar. Bir cihaz 802.11g veya 802.11b bir veriyi ileteceği zaman öncelikle gideceği yere bir RTS mesajı yollar. Gönderici alıcıdan cevap bekler. Alıcıdan CTS mesajı alınınca, iletimin başlaması gerektiğini anlar. Alıcı göndericiye CTS yollarken, mesajı yayar ve böylelikle ağdaki diğer cihazlar aynı zamanda başka mesaj göndermemeleri gerektiğini anlar. Farklı bir koruma mekanizması olan CTS to Self, bir kısım veri gönderilmek istendiği zaman erişim noktası tarafından kullanılır. Bu mesaj RTS mesajı olmadan yollanır. [14][15]

2.3. 802.11 YEREL ALAN AĞLARINDA GÜVENLİK

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

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

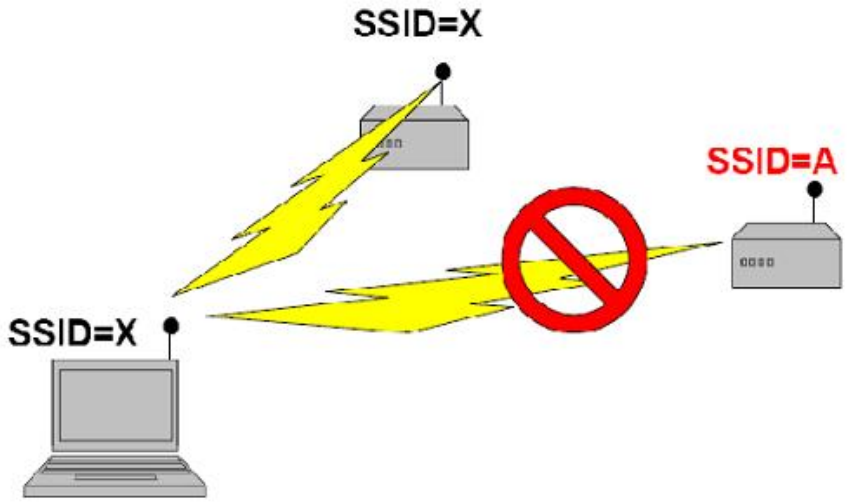
Kronolojik sıra ile ilk olarak WEP algoritması geliştirilmiştir. WEP algoritmasının kullanıma başlaması ile birlikte önemli güvenlik açıkları tespit edilmiştir. Bu açıkları gidermek için iki aşamalı bir çözüm başlatılmıştır. Uzun vadeli olan çözüm IEEE tarafından oluşturulan bir çalışma grubu 'TGi' tarafından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

2.3.1. Geleneksel WLAN Güvenliği

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

802.11 standardı SSID'yi kullanıcı belirli bir kablosuz LAN'a katılmak istediğinde radyo NIC için bir şifre gibi belirler. 802.11, ilişkilendirme işlemi ve diğer cihazlarla iletişim sağlayabilmek amacıyla kullanıcının SSID değerinin Şekil 2.5'ten de görüldüğü gibi erişim noktası ile aynı olmasını gerektirir. Aslında SSID opsiyonel güvenlik özelliklerinin yokluğunda erişim noktalarının ilişkilendirme işlemi için gerek duyduğu tek güvenlik mekanizmasıdır.

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

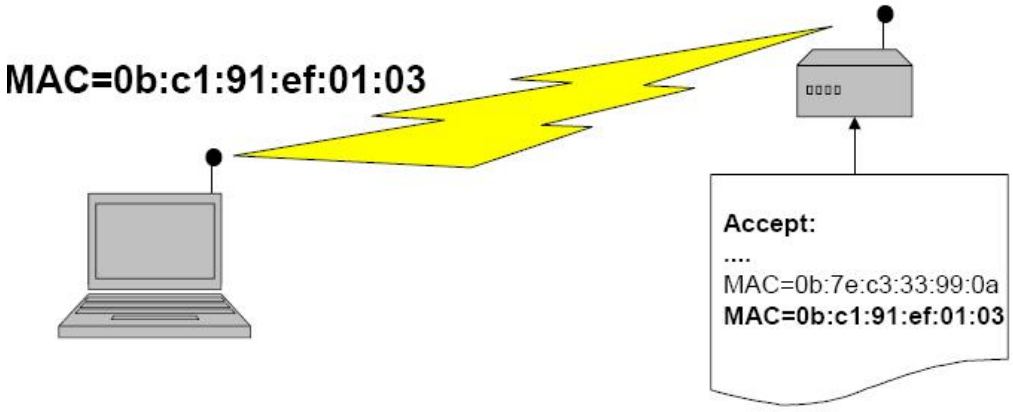


Şekil 2.5 : SSID Kullanımı

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

2.3.1.2. MAC Adresi Filtreleme

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



Şekil 2.6 : MAC Adresi Filtreleme İşlemi

MAC adresi filtreleme ağa erişimi belirli MAC adreslerine izin vermek suretiyle sınırlar (Şekil 2.6). Ancak bu metodun bir çok dezavantajları vardır. Öncelikle istemcilerin MAC adresleri kolaylıkla değişebilir ve böylece yetkisi olan bir istemcinin MAC adresinin erişimi engellenebilir. Ayrıca MAC adresleri düzgün metinler olarak gönderildiği için doğru adreslerin ağdan kolayca yakalanması mümkündür. Diğer bir dezanavantaj ise MAC adres filtrelerinin güncel tutulması ve yönetim işlemlerinin oldukça zor olmasıdır. [16][17]

2.3.2. Doğrulama (Authentication)

2.3.2.1. Açık Sistem Doğrulama (Open System Authentication)

Varsayılan olarak düşünülen doğrulama servisidir. Aslında "sıfır" doğrulama anlamına gelmektedir yani hiçbir doğrulama mekanizması bulunmamaktadır. Şekil 2.7'nin adımlarında da görülebileceği gibi ağa bağlanmak isteyen her istemciye katılımı için izin verir.

Şekil 2.7 : Açık Sistem Doğrulama

2.3.2.2. Paylaşılan Anahtarlı Doğrulama

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

Şekil 2.8 : Paylaşılan Anahtarlı Doğrulama

Paylaşılan anahtarlı doğrulama dört aşamada meydana gelir: (Şekil 2.8)

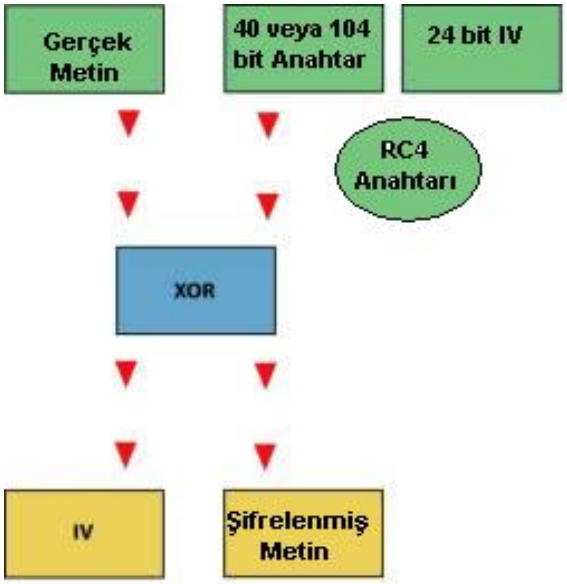
1. Talepte bulunan istasyon AP'ye bir doğrulama çerçevesi yollar
2. AP bu doğrulama çerçevesini alır ve PRNG (pseudorandom number generator) kullanan WEP şifreleme mekanizması tarafından üretilen rasgele bir metinle karşı tarafa cevap verir.
3. Talepte bulunan istasyon bu metini doğrulama çerçevesinin içine kopyalar ve paylaşılan gizli anahtar ile şifreler. Şifrelenmiş çerçeve AP'yeri geri yollanır.
4. Çerçeveyi alan AP metni alır ve aynı gizli anahtar ile deşifreleme yapar. Elde ettiği metni daha önce yolladığı metin ile karşılaştırır
5. Eğer doğru sonucu elde ederse onay yollanır, aksi durumda doğrulama meydana gelmez. [5]

2.3.3. WEP (Wired Equivalent Privacy)

WEP, bir grup IEEE gönüllüsü tarafından 802.11 ağlarda güvenliği sağlamak için geliştirilmiş bir şifreleme algoritmasıdır. WEP algoritmasının amacı radyo sinyalleri ile haberleşen iki son kullanıcı bilgisayarın güvenli bir şekilde haberleşmesini sağlamaktır. WEP geliştirilirken üç hedef belirlenmiştir: [18]

- Kablosuz iletişimin dış güçler tarafında dinlenmesini engellemek (Stopping eavesdropping)
- Yetkilendirilmemiş bağlantı ile ağa erişimi engellemek (Access Control)
- Veri bütünlüğünün bozulmasını engellemek (Data Integrity)

Şekil 2.9'da blok şeması gösterilen WEP algoritması 64 bitlik bir anahtar ve şifreleme için zayıf bir yöntem olan RC4 şifreleme algoritmasını kullanmaktadır. WEP'in kullandığı 64 bit anahtar ise 40 bit WEP anahtarı ve 24 bit başlangıç vektörü (initialization vector - IV) değerlerinin birleşmesinden meydana gelmektedir. Bu 64 bitlik şifre ile gönderilmek istenen metin (plain text) XOR işlemi ile şifrelenmekte ve şifrelenmiş metin (cipher text) elde edilmektedir. Karşı tarafta da şifreleme anahtarı ile şifrelenmiş metin tekrar XOR işlemine tabi tutularak şifre çözülmektedir. [19]



Şekil 2.9 : WEP Algoritması

2.3.2.1. Problemler

WEP, yapısından kaynaklanan birçok ciddi problemi barındırmaktadır ve kablolu ağlara denk güvenilirlik amacına ulaşmamıştır. Ayrıca doğrulama ve bütünlük konularında da beklenen amaçlara ulaşamamaktadır.

WEP temel olarak iki büyük sorun içermektedir. Bunlardan ilki WEP'in kullanımın isteğe bağlı olması ve sonucunda da birçok gerçek uygulamada şifrelemenin hiçbir zaman kullanılmamış olmasıdır. Diğeri ise varsayılan olarak WEP'in tüm WLAN kullanıcıları için tek bir gizli anahtar kullanır ve bu ortak anahtar her cihazda erişilebilir bir ortamda tutulur. Eğer herhangi bir cihaz kaybolursa ya da çalınırsa geri kalan tüm cihazların gizli anahtarlarının değiştirilmesi gerekir. Ayrıca WEP bir anahtar dağıtım protokolü içermediği için yeni anahtarların dağıtımı da oldukça zor bir süreçtir. Sonuç olarak da anahtar uzlaşması çok kere yok sayılır. Tüm bu durumlar sonucunda WLAN ortamlarında güvenilirliği ve bütünlüğü sağlamak oldukça zor hale getirmektedir. [20]

Pratikte WEP'in doğurduğu en büyük sorun WEP anahtarlarının kripto analizler sonucunda elde edilebilmesidir. Ağustos 2001'de Fluhrer, Mantin ve Shamir WEP'in 64 bit anahtar oluşturma mekanizması üzerine yeni bir saldırı tanımlamışlardır.[21] İçerdikleri metnin ilk baytı bilinen milyonlarca şifrelenmiş paketi elde edebilen bir saldırgan RC4 anahtar zaman çizelgesini kullanarak temel RC4 anahtarını elde

edebilmektedir. Kısa bir süre sonra Stubbfield, Ioannidis ve Rubin yeni bir saldırı gerçekleştirmişler ve gerçek sistemlerin de kırılabileceğini göstermişlerdir. [22] Gerekli şifrlenmiş paketlerin elde edilebilmesi için ağın birkaç saat dinlenmesinin yeterli olacağını belirlemişlerdir. Daha sonra da Fluhrer-Mantin-Shamir (FMS) saldırısı kullanılarak WEP ile korunan ağların kırılması işlemini otomatik olarak gerçekleştiren araçlar gelmektedir.

Bir FMS saldırısı WEP'in yapısını yıkar ve WEP anahtarı bir kez elde edildiği zaman tüm güvenlik yok olur. Bu durumda oluşabilecek güvenlik riskleri şunlardır:

- Saldırgan karşılaştığı paketlerin deşifre edebilir ve şifrelenemiş trafiği okuyabilir. Bu WEP'in gizlilik amaçlarına ters düşer.
- Saldırgan WEP'in bütünlük ve doğrulama esaslarına ters düşecek şekilde AP tarafında kabul edilebilir yeni ve sahte şifrelenmiş paketleri yayınlayabilir, kablosuz ağa katılabilir veya diğer bilgisayarlara saldırabilir.

FMS saldırısı ve onu takip eden çalışmalardan daha önce kriptograflar da WEP ile ilgili bir çok sorunu ortaya çıkarmışlardır. Örneğin 2000 yılında Walker [23] kısa IV uzunluğunun anahtar dizilerinin tekrar üretimi için risk oluşturduğunu ve bunun da ağı dinleyen bir saldırganın şifrelenmemiş metni ele geçirebileceğini belirtmiştir. Daha sonra Ocak 2001'de Borisov, Goldberg ve Wagner birkaç farklı saldırı göstererek bir saldırganın ilk olarak doğrulama protokolünün devre dışı bırakıp ve tespit edilme korkusu olmadan şifrelenmiş metinlerin üzerinde kolayca değişiklik yapabileceği gerçeğini ortaya koymuşlardır. [24] Daha sonra Arbaugh bu fikri pratikte bir saldırganın seçilen herhangi bir paketi birkaç saat içinde deşifre edebileceği bir saldırıya dönüştürmüştür. [25]

Özet olarak WEP'in yapısından kaynaklanan problemler şu şekilde tanımlanabilir: [20]

- 24 bit IV çok kısadır bu gizlilik esasını riske atmaktadır.
- CRC kontrol toplamına Bütünlük Kontrol Değeri (Integrity Check Value-ICV) adı verilir ve WEP tarafından bütünlük koruması için kullanılır. Bu güvenli olmayan bir yöntemdir ve elde edilen paketleri verilerin değiştirlmesine karşı korumaz.

- WEP, IV değerini anahtar ile kriptoanalitik saldırılara uygun şekilde birleştirir. Sonuç olarak da pasif saldırganlar birkaç milyon paketi elde ettikten sonra anahtarı elde edebilirler.
- Kaynak ve hedef adresleri için bütünlük kontrolü WEP tarafından sağlanmaz.

2.3.2.2. Wep'in Güvenlik Önlemlerini Arttırmak Için Yapılmış Olan Çalışmalar

WEP'in güvenlik problemlerinin tespit edilmesinin ardından firmalar öncelikle bu güvenlik problemlerini aşmak için kendileri çeşitli yöntemler denemişlerdir. Bu çalışmalar şu şekildedir :

- Genişletilmiş WEP Anahtarı

Lucent firması tarafından 1998 yılında WEP anahtarı 128 bit olacak şekilde WEP protokolü yeniden düzenlemiştir. Bu çalışmada 128 bitlik anahtar yine 24 bitlik bir IV içermektedir. Sonuç olarak WEP anahtarının genişletilmesi ile saldırganların şifreyi kırmak için toplamaları gereken örnek sayısı ve harcamaları gereken zaman arttırılmıştır. Bu gelişmeyi takiben Agere ve U.S.Robotics firmaları da sırası ile 152 bitlik ve 256 bitlik WEP anahtarlamalı protokolleri oluşturmuşlardır.

- Dinamik WEP Anahtarı

Dinamik WEP Anahtarı çalışması Cisco ve Microsoft'un da aralarında bulunduğu çeşitli firmalar tarafından geliştirildi. AP'ler aracılığı ile yayılması planlanan kısa süreli ve sistem mühendisinin belirleyeceği zaman aralıklarında WEP anahtarının değiştirilmesini öngören bir protokoldür. Bu protokol değişikliği ile saldırganlara şifreyi kırıp sisteme zarar verme zamanı tanımadan WEP anahtarını değiştirmek amaçlanmaktadır.

- VPN Uygulaması

VPN (Virtual Private Network) ile bilgilerin özel bir kanal ile güvenli bir şekilde taşınması mantığı geliştirilmiştir. Bu yöntem güvenlikle ilgili problemleri büyük ölçüde kontrol altına alsa da roaming işlemi sırasında hatalar oluşmuş ve problemler ortaya çıkmıştır.

Çeşitli firmalar tarafında geliştirilen tüm bu gelişmeler WEP'in doğasında bulunan problemleri çözememiştir ve sadece geçici çözümler olabilmişlerdir. [19]

2.3.2.3. Saldırı Türleri

- Zayıf Nokta IV Saldırısı

Zayıf IV saldırısı , RC4 algoritmasının zayıf uygulamasına bağlı olup, ilk kez Fluher, Mantin&Shamir tarafından farkedilmiştir. [6] Saldırının değerini anlamak için iki parametre düşünülmelidir. Bunlardan ilki zaman ve saldırıyı uygulamada gerekli efor, diğeri de ağ üzerinden sahip olacağımız çarpışma etkisidir. Bu saldırı uygulamada çok fazla efor gerektirir, fakat çıkış, ağa tamamen tüm kapıları açan gizli anahtardan keşfedilir .

WEP'in yetersizliği ortaya çıktığı için, otomatik olarak gizli anahtarı kırabilme durumuna da dikkat edilmesi gerekir. Bu amaç için iki araç var WEPCrack [8] ve AirSnort [9] ve bu ikisi de kullanılabilir. Böylece herkesin ihtiyacı olan tek şey , gerekli yamalarla doğru OS ve NIC'e sahip olmaktır. Yeterli paket ve araç yakalandığında bu gizli anahtara dönüşecektir.

RC4 anahtar çizelgelemesinin anlatıldığı orijinal makalede şöyle bahsedilmektedir: "Gerçek bir WEP bağlantısına saldırmaya teşebbüs edemeyiz ve bu yüzden WEP in bu saldırılara karşı savunmasız olduğunu iddia edemeyiz." Fakat AT&T Laboratuvarlarında [10] yapılan bir araştırmaya göre bu saldırılar uygulanmış ve pasif bir saldırı ile bu 128 bitlik anahtar keşfedilebilmiştir.

WEP şifrelemesinin zayıf noktası başlangıç vektörünün kötü kullanımından ileri gelmektedir. Örneğin bir hacker aynı başlangıç vektörünü kullanan iki veri paketini yakalar ve bunları XOR fonksiyonunu kullanarak matematiksel olarak birleştirirse, bir anda anahtarı elde edebilmektedir. Bu saldırı tipi , anahtar akışının ilk çıktı kelimesini bulma fikrine dayanır ve bu mesajın ilk şifrelenen değerinin bilinmesini gerektirir. Genellikle IP ve ARP gibi bilinen başlıklara sahip ağ üzerindeki birçok trafikte kullanılabilir.

- IV Çakışması

IV çakışması aynı gizli anahtar ve IV ile şifrelelen iki farklı paketin saldırgan tarafından yolunun kesilmesi anlamına gelmektedir. Bu mesajlardan gizli anahtar bilgisi bilinmeksizin içerik hakkında bilgi elde edebilir. RC4 anahtar akışı bu paketler için

aynıdır ve bu yüzden iki mesajın birbiri ile arasında gerçekleştirilen XOR işlemi ile gerçek metin elde edilir. C1=Ciphertext, k=key, IV= Initialization Vector, P1=Plaintext1 ve P2=Plaintext2 olmak üzere aşağıdaki işlemler aşağıdaki gibi gösterilebilir:

If

$C1=P1 \oplus RC4(IV,k)$

$C2=P2 \oplus RC4(IV,k)$

Then

$C1 \oplus C2= P1 \oplus P2$

Yukardaki sonuç düşünüldüğünde bu basit saldırı gerçek mesaj metni bilindiğinde mümkün olmaktadır. Gerçek mesaj bilindikten sonra diğer mesaj kolaylıkla bulunabilir. Genelde saldırgan çok şanslı olmaz ve aktif saldırıda bulunmadıkça mesajın tüm içeriği hakkında bilgiye sahip olamaz. Fakat bu bilginin kullanılamayacağı anlamına gelmez. XOR sonucunun bilinmesiyle her bir mesajı tahmin edebilecek bir çok yol mevcuttur.

Bu tip saldırıların başlangıç noktası IV çakışması (tekrar kullanımı) örneğinin bulunması ile başlar. WEP her paket için IV'nin değiştirilmesini önerir, fakat IV'nin oluşturulması için özel bir yöntem bulunmamaktadır. Kısa IV uzunluğu çakışmaları kaçınılmaz hale getirmektedir fakat bazı uygulamalar bu çakışma olasılığını daha fazla arttırmaktadır. Örneğin 5 Mbps ile çalışan bir 802.11b erişim noktasında, ortalama paket boyutu 1500 bayt olsun. Bu durumda tüm olası 24 bit IV değerleri yaklaşık on saat içerisinde kullanılacak demektir.

- Mesaj Modifikasyonu

Ağda gönderilen mesajların bütünlüğünün kontrol edilmesi alıcıda CRC-32 kontrol toplamı hesaplanması gerçekleştirilir ve göndericinin eklendiği değer ile karşılaştırılır. Bu rastgele oluşan hataları tanımlamada etkili bir yoldur, fakat bu iyi bir saldırgan mesaj içeriğini değiştirmeden asla alıkoymaz.

CRC kontrol toplamının doğrusal olması nedeniyle orjinal mesajımızı (M) istediğimiz mesaja (M1) dönüştürebiliriz. Bunun için XOR işlemi ile M mesajını M1'e dönüştüren X akışınının bulunması gerekmektedir.

$$M1 = M \oplus X$$

Eğer M'in kontol toplamını C, M1'in kontrol toplamını C1 ile ve X in kontrol toplamını CX ile gösterirsek, elde ettiğimiz şifreli mesajı <X,CX> ile XOR işlemine tabi tutarsak , alıcının bu mesajı bizim istediğimiz M1 mesajı şeklinde deşifre etmesini sağlamış oluruz.

Aşağıdaki adımlar bu işlemleri göstermektedir:

$$(RC4(IV,k) \oplus <M,C>) \oplus <X,CX>$$
$$= RC4(IV,k) \oplus (<M,C> \oplus <X,CX>)$$
$$= RC4(IV,k) \text{ c}(<M \oplus X, C \oplus CX>)$$
$$= RC4(IV,k) \oplus <M1,C1>$$

Elde edilen sonuç değiştirdiğimiz M1 mesajının da doğru CRC değerini verdiğini göstermektedir. (M ⊕ X) ve (C ⊕ CX) işlemlerinin kontrol toplamı değerleri CRC işleminin XOR işlemi üzerinde dağılma özelliğine sahip olmasından dolayı eşittir.

Bu modifikasyonda istenilen amaca ulaşmak için saldırgan orijinal mesajı veya en azından değiştirmek istediği alanı bilmek zorundadır. Saldırganın gerçek metni elde edebilmesi için erişim noktasını da kullanabiliyor olmasından dolayı bu aktif bir saldırıdır.

- Mesaj Enjeksiyonu

WEP IV seçme kurallarını tanımlayamamıştır ve her paket için bir IV oluşturulmasını tavsiye eder, fakat birçok mesaj için tek bir IV'nin kullanılma durumu hala vardır. Algoritmadaki bu açık nedeniyle, aktif bir saldırgan tek bir anahtar akışı yakaladığında ağ içine mesaj enjekte edebilir.

Bu saldırganın daha önce bahsettiğimiz metotlardan biri veya başka metot ile tek bir anahtar akışını yakalamsı durumunda , WEP tarafından sağlanan erişim kontrolünü geçer ve ağ üzerinde iletişim yapabilir. WEP IV'nin her pakette değişmesinin gerekliliğini kesin olarak belirtmediği için erişim noktası paketi kabul eder ve herhangi bir hata durumu tetiklenmez.

Mevcut standartın özelliğinden dolayı bilinen bir anahtar akışı kullanılarak yeni mesajlar kolaylıkla oluşturulur. İstenilen mesaj için CRC kontrol toplamı hesaplanır ve mesaja eklenir. Daha sonra da bu bilinen anahtar akışı ile mesaj deşifrelenir. Bunu durdurmanın bir yolu anahtarlı mesaj doğrulamasını (keyed message authentication) kullanmaktır ve bu metot 802.11i taslağında yer almaktadır.

- Diğer Saldırılar

WEP'e yapılabilecek birçok aktif saldırı bulunmaktadır. Bu aktif saldırılar genellikle daha önce bahsettiğimiz pasif saldırılarla aynı özelliklere sahiptir. Birkaç aktif saldırı önlense de, hala ağ güvenlik köprüsünü geçmekte gerek duyulan parametrelerin oluşturulması için birçok metot mevcuttur.

Bernard Aboba [12] tarafından yapılan bir çalışmada bazı olası saldırılardan bahsedilmiştir. Bu olası saldırı senaryoları topoloji, trafik tipi ve diğer parametrelerle birlikte değişiklik göstermektedir. Fakat birçok aktif saldırının temelinde daha önce bahsettiğimiz bir saldırı türünün yattığını görebiliriz.

Bilinen gerçek metin saldırısı bilinen bir mesajın kullandığı anahtar akışının elde edilmesine dayanır. Kısmi bilinen gerçek metin saldırısı da aynı fikre dayanır. Anahtar akışının bazı kısımları elde edilir, Bu işlemin sürekliliği sağlanırsa elde edilen anahtar akışının uzunluğu arttırılabilir.

Tepkime saldırıları, mesajı bit bit keşfetmek için TCP trafiğinin TCP kontrol bileşeni alanını kullanır. Bu mesajı değiştirme ve alıcıdan mesaj hakkında bilginin elde edilebileceği bilgi mesajını bekleme işlemidir. Bu işlemin tekrarlanması ile gerçek metin mesajı elde edilir. DoS (Denial of Service) , Oturum Bozma (Session Hijacking) ve benzer saldırılar da WEP sistemlerine gerçekleştirilebilir. [24]

2.3.4. WPA (Wi - Fi Protected Access)

WEP algoritmasının açıklarını gidermek için IEEE çalışma grupları tarafından çalışmalar yapılmış ve biri kısa vadeli diğeri ise uzun vadeli olmak üzere iki farklı çözüm üretilmiştir. Uzun vadeli olan çözüm IEEE'nin "i" çalışma grubu tarafından tam olarak güvenli bir protokolün oluşturulması şeklindedir. Bu çalışmalar esnasında sektörün WEP algoritmasındaki güvenlik zaaflarından etkilenmemesi ve biraz da olsa güvenlik önlemlerinin arttırılması için WEP algoritmasının eksik yönlerinin geçici yöntemlerle giderilmesi için Wi-Fi grubu ve IEEE tarafından WPA geliştirilmiş ve sektör için geçici bir çözüm üretilmiştir. WPA'nın geliştirilmesiyle eski donanımın sadece yazılım güncelleştirilmeleri yapılarak kullanılabilmesi sağlanmıştır. Var olan donanımın kullanımı ile WPA'nın kullanımının daha kolay bir şekilde ve daha hızlı bir şekilde yayılması sağlanmıştır.

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

WPA'da kullanılan şifreleme algoritması tıpkı WEP gibi RC4 algoritmasına dayanan Geçici Anahtar Bütünlük Protokolü (Temporal Key Integrity Protocol - TKIP) 'dür. TKIP WEP'ten farklı olarak önemli bazı değişiklikler içermektedir. IV'nin uzunluğu 24 bitten 48 bite çıkarılmıştır ve şifreleme anahtarları her oturumda değiştirilmektedir. Ayrıca her paket için farklı anahtar kullanımını sağlamak amacıyla da bir anahtar karıştırma fonksiyonu (key mixing function) kullanılmaktadır. WPA iletim sırasında verilerin değişikliğe uğramamasını sağlamak amacıyla da Michael adı verilen bir mesaj bütünlük kodu (message integrity code - MIC) kullanır. [26]

2.3.5. WPA2 (802.11i)

TGi tarafından kablosuz ağların güvenliği için uzun vadeli çözüm olarak düşünülen WPA2 Mayıs 2004 tarihinde standart haline gelmiş ve Ekim 2004 tarihinden itibaren de

bu protokolü destekleyen ürünler üretilmeye başlanmıştır.WPA2 ayrıca IEEE 802.11i olarak da adlandırılmaktadır. WPA günümüzde kırılmamış olsa da WEP tabanlı bir yapı olduğu ve eksiklerinin çıkabileceği şüphesinden dolayı (RC4 algoritmasının zayıflıkları) IEEE tarafından geliştirilen bu protokol WPA'nın aksine WEP üzerine kurulmamış, yeni ve farklı bir yapı olarak geliştirilmiştir. WPA2'nin WPA ve WEP'ten en büyük farkı ağ trafiğini şifrelemek için RC4 algoritmasını değil AES (Advanced Encryption Standart) [27] algoritmasını kullanmasıdır.

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

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

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

- Önceden Doğrulama: Önceden doğrulamada kullanıcı bir erişim noktasına bağlı iken diğer bir erişim noktasının varlığının farkına varırsa 802.1X anahtar değişimi ile bu erişim noktası için de anahtarları elde eder ve saklar. Sinyal zayıflığı gibi nedenlerden önceden anahtarını elde ettiği erişim noktasına geçmek isterse 802.1X işlemleri tekrar yapılmaz
- Anahtar önbellekleme: Erişim noktası ile daha önceden anahtar belirleme işlemi gerçekleşmiş ise bu anahtarlar bellekte saklanır. Bu erişim noktası ile iletişime geçildiğinde 802.1X işlemleri tekrar yapılmaz. [19][26]

Tablo 2.2 : WEP-WPA-WPA2 Sistemlerinin Karşılaştırması

	WEP	**WPA**	**WPA2**
Şifreleme	Şifreleme yapısı kırıldı. RC4 algoritması	WEP in açıklarını kapatıyor. TKIP/RC4	CCMP/AES CCMP/TKIP
Şifreleme Anahtarı	40 veya 104 bit	128 bit	128 bit
IV	24 bit	48 bit	48 bit
Anahtar Değişikliği	Anahtar sabittir.	Anahtarlar her oturum,her paket için değişir.	Anahtar değişikliğine gerek yoktur.
Anahtar yönetimi	Anahtar yönetimi yoktur	802.1X	802.1X
Doğrulama	Zayıf bir yöntem	802.1X EAP	802.1X EAP
Veri Bütünlüğü	CRC	Michael	MIC

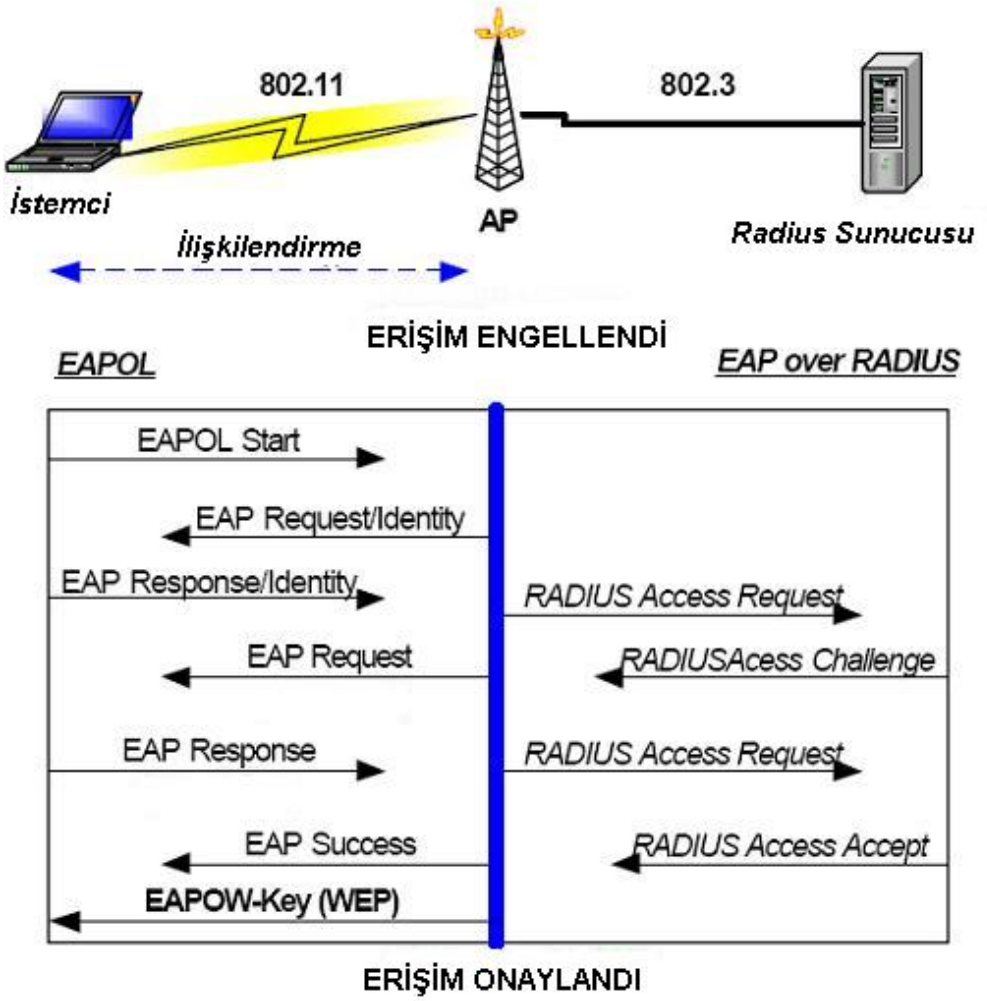
2.3.6. 802.1X

802.1X doğrulama protkolü kablolu ağlar için geliştirilmesine karşın kablosuz ağlar için de kullanılmaktadır. Bu protokol, istemci ile erişim noktası arasında bir doğrulama sunucusu (authentication server) kullanarak doğrulama ve port-tabanlı erişim kontrolü sağlamaktadır. Temel olarak 802.1X standardı 3 elemandan oluşmaktadır:

- Kullanıcı (supplicant): Doğrulama isteğinde bulunan kullanıcıdır.
- Doğrulama Sunucusu (Authentication Server): RADIUS gibi doğrulama hizmetleri için bir sunucu.
- Doğrulayıcı (Authenticator): Kullanıcı ile doğrulama sunucusu arasındaki birimdir ve genellikle erişim noktasıdır.

Doğrulama süreci aşağıdaki işlemlerden oluşur:

1. Kullanıcı, doğrulayıcıya bağlantı talebinde bulunur. Doğrulayıcı, bağlantı talebini alınca, tüm portları kapalı tutar fakat kullanıcı ile arasında bir port açar.
2. Doğrulayıcı, kullanıcıdan kimliğini (identity) ister.
3. Kullanıcı kimliğini gönderir. Doğrulayıcı kimlik bilgisini bir doğrulama sunucusuna gönderir.
4. Doğrulama sunucusu, kullanıcının kimliğini doğrular. Doğrulandığında, Kabul (Accept) mesajı doğrulayıcıya gönderilir. Doğrulayıcı, kullanıcının portunu yetkilendirilmiş duruma getirir.
5. Kullanıcı, doğrulama sunucusundan, sunucunun kimliğini ister. Doğrulama sunucusu, kimlik bilgisini kullanıcıya gönderir.
6. Kullanıcı, doğrulama sunucusunun kimliğini doğruladığında, veri trafiği başlar. [28]



Şekil 2.10 : 802.1X Doğrulama Mekanizması

Doğrulayıcı, kullanıcı ve doğrulama sunucusu arasındaki iletişimi sağlamak için Genişletilebilir Doğrulama Protokolünü (Extensible Authentication Protocol - EAP) kullanmaktadır. EAP her bağlantı katmanında çalışabilen ve RADIUS gibi herhangi bir doğrulama mekanizmasını kullanmak üzere dizayn edilmiş bir sarmalama (kapsülleme) mekanizmasıdır. EAP mesajlarının kendileri kapsüllenmiş şekildedir. EAP over LAN (EAPOL) kapsüllemesi EAP çerçevelerini kullanıcı ve doğrulayıcı arasında taşır ve kriptografik anahtar bilgilerinin taşınmasında kullanılabilir. EAP ve EAPOL protokollerinin her ikisi de bütünlük kontrolü veya gizlilik koruması ile ilgili herhangi bir önlem içermez. Doğrulama sunucusu ve doğrulayıcı ise aralarında EAP over RADIUS protokolü ile haberleşir. Bu mekanizma Şekil 2.10'da adım adım gösterilmiştir. RADIUS protokolü doğrulayıcı ve sunucu arasında HMAC-MD5 ve paylaşılan benzersiz bir anahtar kullanarak her paket için doğruluk ve bütünlük sağlar. [9] [29]

WLAN ortamında kablosuz istemci kullanıcı , erişim noktası doğrulayıcı, RADIUS sunucusu ise doğrulama sunucusu konumundadır. (RADIUS dışında diğer doğrulama mekanizmaları da kullanılabilir.)

802.1X'in adımları başlamadan önce normal 802.11 ilişkilendirme sürecinin tamamlanmış olması gerekir çünkü, 802.1X aktif durumda bir bağlantı gerektirmektedir. Başarılı 802.1X doğrulamasından önce AP tüm 802.1X-olmayan trafiği iptal eder. 802.1X değişimi boyunca RADIUS sunucusu istemciye bir davet yollar. İstemci kullanıcı tarafından sağlanan şifreyi bu davete bir cevap üretmek için kullanır ve bunu erişim noktası aracılığıyla sunucuya yollar. RADIUS sunucusu bünyesinde bulundurduğu veritabanından kullandığı bilgiler ile kendi cevabını üretir ve bunu istemcinin yolladığı cevap ile karşılaştırır. Eğer eşitse doğrulama başarılı bir şekilde gerçekleşmiş demektir. Başarıyla gerçekleşmiş doğrulamadan sonra RADIUS sunucusu dinamik bir WEP anahtarı üretir. Sunucu bu gizli WEP anahtarını erişim noktasına yollar. İstemciye WEP gizli anahtarının iletilmesi için EAPOL anahtar çerçeveleri kullanılır. Bu yapı periyodik olarak anahtarları dinamik olarak değiştirmek için kullanılabilir. Elde edilen her kullanıcı ve her oturum için farklı WEP anahtarlarıdır. [29]

3. MALZEME VE YÖNTEM

3.1. RC4 ALGORİTMASI

RC4 yazılım uygulamalarında en geniş uygulama alanına sahip olan şifreleme algoritmalarından biridir. İlk kez 1987 yılında Ron Rivest tarafından geliştirilmiştir [30] ve 1994'te ortaya çıkana kadar ticari bir sır olarak saklanmıştır. Buradaki amaç; verilen bir gizli anahtar ile geniş uzunlukta rasgele sayılar üretmek ve daha sonra bu akışla düz metin mesajı şifrelemektir. Alıcı verilen anahtarla aynı akışı üretebilecek ve alınan mesaj deşifrelenecektir. Mesajın deşifreleme ve şifrelemesi temel olarak XOR fonksiyonu ile yapılmaktadır.

RC4 iki bölümden oluşmaktadır :

- Anahtar Planlama Algoritması (Key Scheduling Algorithm - KSA) : Tipik olarak 40 bit ile 256 bit arasında uzunluğa sahip olan anahtarı bir başlangıç S permütasyonuna dönüştürür.
- Çıkış Üretme Parçası (Output Generation Part - PRGA) : Üretilen permütasyonu kullanarak bir sahte-rasgele çıkış dizisi üretimini gerçekleştirir. [21]

3.1.1. Anahtar Planlama Algoritması (KSA)

(K) anahtarının KSA'ya L kelime olarak verildiğini ve her bir kelimenin n bitten oluştuğunu düşünelim. N muhtemel kelime değerlerinin sayısı olmak üzere başlangıç permutasyonu S{0,...,N-1} aşağıda verilen adımlara göre K anahtarından türetilmiştir.

KSA (K)

Başlangıç:

For i = 0…N -1

S[i] = i

i = 0

Şifreleme:

For i = 0…N-1

j = j + S[i] + K [i mod L]

Swap (S [i] , S [j])

KSA, başlama periyodu boyunca tüm muhtemel kelime değerleri dizisini oluşturmasıyla başlar. Bir sonraki adımda şifreleme bölümünde bu dizinin içeriği rasgele sıralanmış değerler ile değiştirilir. Her adımda dizinin i indeksi bir arttırılır ve her adımda j indeksi hesaplanır ve burada KSA'ya giriş olan K anahtarı kullanılır.

3.1.2. Çıkış Üretme Parçası (PRGA)

Anahtar planlama algoritmasının tamamlanmasından sonra olası tüm n bit kelimelerin bir dizisine rasgele sıralanmış halde sahip olunur. Bir sonraki adım bu diziyi kullanarak rasgele ve uzun kelimeler akışları üretmektir. Bu üretim algoritması (PRGA) aşağıdaki gibidir:

PRGA(K)

Başlangıç:

i = 0

j = 0

Üretme döngüsü:

i = i +1

j = j + S[i]

Swap (S[i] , S[j])

Output z = S [S [i] + S[j]]

PRGA üretme döngüsü, veriyi şifrelemede kullanılacak n bitlik rasgele çıkış kelimeleri üretmek için kullanılmaktadır. Her bir döngüde i indeksi bir arttırılır ve ilk N adımda dizi taranacak ve her bir eleman bu zaman en az bir kez takas edilecektir.

WEP'te kullanılan RC4 gerçeklemesinde her bir kelime 8 bit (=n) ve olası değerlerin toplam sayısı olan 256 (=N) aynı zamanda KSA tarafından oluşturulacak dizi uzunluğudur. Orjinal WEP de kullanılan KSA'ya giriş olan anahtar uzunluğu genelde 64 bittir ve bu 8 kelimeye eşittir. Ayrıca 128 bitlik uzun anahtar kullanan uygulamalar da mevcuttur.

KSA'da kullanılan anahtarların iki kısmı vardır; birincisi ağ yöneticisi tarafından belirlenen gizli anahtar diğeri ise istasyon tarafından oluşturulan rasgele sayıdır. WEP güvenliğinin altında yatan problem bu değerlerin oluşturulması için herhangi bir metodun bulunmamasından ve bunların iletimin hava yoluyla gerçekleşmesinden kaynaklanmaktadır.

3.2. WEP ALGORİTMASI

WEP algoritması 64 bitlik bir anahtar ve şifreleme için zayıf bir yöntem olan RC4 şifreleme algoritmasını kullanmaktadır. Bu 64 bitlik şifre ile gönderilmek istenen metin (plain text) XOR işlemi ile şifrelenmekte ve şifrelenmiş metin (cipher text) elde edilmektedir. Karşı tarafta da bir metnin iki defa aynı anahtar ile şifrelenmesi sonucu kendisinin elde edilmesi prensibine göre şifre çözülmektedir. WEP'in şifreleme mantığı kısaca bu işleme dayanmaktadır.

WEP güvenliğini kullanan WLAN sistemlerinde tüm sistemdeki bilgisayarlara dağıtılmış bir 40 bitlik WEP anahtarı bulunmaktadır. Bir metin şifrelenip gönderilmek istenirse bu WEP anahtarı ile 24 bitlik rastgele seçilen bir IV birleştirilerek 64 bitlik bir anahtar oluşturulur. IV'nin kullanılma sebebi, WEP anahtarının ağdaki tüm bilgisayarlarda olması ve bir diğer bilgisayarın bizim gönderdiğimiz mesajı rahatlıkla okumasına engel olmaktır. Oluşturulan bu 64 bitlik anahtar ile veri şifrelenir ve şifrelenmiş veri ile birlikte IV bir paket halinde ilgili bilgisayara gönderilir. Gönderim sırasında IV şifrelenmemiş durumdadır. Hedef bilgisayar zaten WEP anahtarına sahip olduğu için gönderilen IV ile şifre çözme anahtarını elde etmiş olur ve gönderilmek istenen metni elde eder.

Algoritmanın bu şekilde çalışmasında çeşitli açıklar bulunmaktadır. Her ne kadar acemi bir şifre kırıcıyı engellese de uzman bir kişi tarafından şifre kolaylıkla kırılabilmektedir. WEP algoritması kırılabilir bir algoritma olarak bilinmektedir.

3.2.1. WEP Anahtar Biçimi

KSA'da kullanılan RC4 anahtarı ağ yöneticisi tarafından sağlanan gizli bir anahtardan ve NIC (Ağ Arayüz Kartı) tarafından oluşturulan ve IV adını verdiğimiz bir numaradan oluşur. Her bir paket için farklı bir IV kullanılması 802.11 standardı tarafından tavsiye edilmektedir. Bu genelde bunu yapan özel bir metot bulunmamasına rağmen bu işlem bir sayaç kullanılarak yapılabilmektedir. IV gizli anahtardan önce yer alır ve böylece 40 bit WEP gizli anahtarı ve 24 bitlik IV anahtar biçimi Tablo 3.1'deki gibidir:

Tablo 3.1 : WEP Anahtar Biçimi

K[0]	K[1]	K[2]	K[3]	K[4]	…	K[7]
IV[0]	IV[1]	IV[2]	k[0]	K[1]	…	k[4]

Yukarıda gösterilen anahtar rasgele akış üretip, mesajı şifrelemek için RC4 tarafından kullanılır. Çünkü her bir mesaj tarafından farklı bir IV oluşturulur ve alıcının bu değeri bilmesi mümkün değildir ve mesajı deşifrelemek için aynı RC4 akışı oluşturulur. Böylece, IV mesajla anlaşılır biçimde iletilir. Fakat burada bir güvenlik tehdidi yatar, yollanan IV demek , saldırganların KSA'ya verilen anahtar ile ilgili kısmi bilgiye ulaşması demektir. Anahtar planlama algoritmasının içerdiği bu zayıflıklara bu çalışmada değinilmeyecektir.

3.2.2. WEP Çerçeve Biçimi

Orjinal 802.11 standardına göre bir WEP çerçevesi sadece iki tanesi şifrelenen dört kısımdan oluşmaktadır.

1. Veri: Bu alanın önceden tanımlanmış bir boyutu yoktur ve üst katman bilgilerini içerir ve şifrelenir.
2. CRC-32: Bu değer alınan verinin bütünlüğünü kontrol etmede kullanılır ve 32 bittir. Veriye eklenir ve onunla şifrelenir.
3. IV : Başlangıç Vektörü 24 bittir ve şifrelenmeden yollanır.

4. Pad & Anahtar ID: Bu iki alan tek bir bayt ve bu bayt'ın iki MSB (Most Significant Bit) değerini oluşturur. Anahtar ID maksimum dört farklı anahtar ile mesajın şifrelenmesini sağlayan gizli anahtarı tanımlar. Pad değeri sıfırdır.

WEP çerçevesinin genel yapısı Tablo 3.2'de gösterilmektedir.

Tablo 3.2 : WEP Çerçevesi

Şifrelenmeden Gönderilen Kısım		Şifrelenen Kısım	
IV(3 Bytes)	Pad &Pad ID (1 Byte)	Data(>=1 Byte)	CRC-32(4 Bytes)

3.2.2.1. CRC-32 (Cyclic Redundancy Check –32)

Dönüşsel Artiklik Denetimi (CRC) bir hash fonksiyonudur ve bir ağ trafiğindeki paket veya bilgisayar sistemlerinin blok dosyaları gibi büyük miktarda veri bloklarından küçük bir kontrol değeri üretir. Bu değeri depolama veya iletim sırasında meydana gelen hataları kontrol etmek için kullanır. CRC gerçeklemesinin basit olması ve matematik olarak analizin kolay olması nedeniyle popüler bir metottur. İletim kanallarındaki gürültüden kaynaklanan sık rastlanan hataları tespit etmekte oldukça başarılıdır.

CRC, WLAN sistemlerinde alıcı tarafındaki verinin bütünlüğünün emin olunması amacıyla WEP tarafından da kullanılır. Paketlerin veri kısmınının bir fonksiyonu şeklinde hesaplanır ve bu kısımla beraber veriye yapılan saldırıları durdurmak amacıyla şifrelenir, fakat bunu yapmakta çok da başarılı olmadığı daha doğrusu yetersiz olduğu görülmüştür.

Önceden saptanan uzunluklu veri sabit bir bölenle bölünür ve kalan CRC değeri gibi kullanılır. CRC-32 kullanımında kalanın uzunluğu 32 bittir. Bu kontrol toplamının doğrusallığından dolayı bilgili bir saldırgan mesajı ve CRC değerini işleyebilir. Bu bölümde daha sonra görebileceğimiz gibi, bilgili bir saldırgan mesajı ve CRC değerini alıcının bu mesajı değiştirilmemiş ve doğru bir şekilde kabul etmesini sağlayacak şekilde işleyebilir. [31]

3.2.2.2. Şifreleme

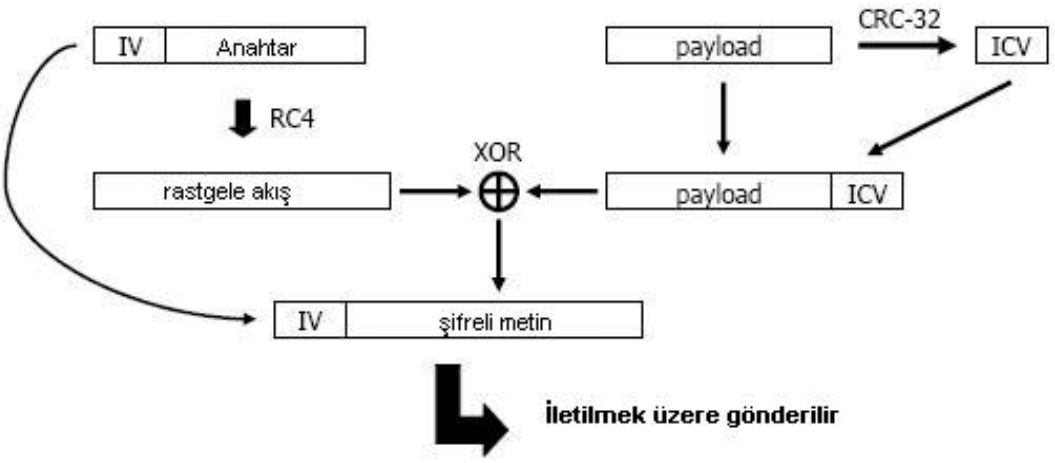
CRC değeri veriye bağlı bir fonksiyon olarak hesaplandıktan sonra verinin yanına eklenir. Her mesaj için gizli anahtar ve IV kullanılarak şifreleme anahtar akışı oluşumu gerçekleştirilir. IV genellikle her paket için bir sayac tarafından özel olarak üretilen 24 bit uzunluğunda bir değerdir. Bu akış, k ve IV ile birlikte RC4 fonksiyonuna giriş olarak kullanılır. (RC4 (IV,k) gibi.)

Veri ve CRC alanları ile anahtar akışı arasında XOR işlemi gerçekleştirilir şifrelenmiş mesaj yani şifreli metin elde edilir.

RC4 şifrelemesinin bileşenleri Tablo 3.3'te, WEP algoritmasının blok şeması ise Şekil 3.1 'de gösterilmiştir.

Tablo 3.3 : RC4 Şifrelemesi

XOR	Gerçek Metin Mesajı	CRC
	Anahtar Akışı= RC4(IV,k)	
IV & Key ID	Cipher Text	



Şekil 3.1 : WEP Algoritması Blok Şeması

Alıcı tarafında ise mesajı deşifrelemek için ilk olarak istasyonda saklanan gizli anahtar ve şifreli mesaj ile birlikte açık bir şekilde yollanan IV değeri kullanılarak anahtar akışı üretilir. Daha sonra şifreli mesaj ile bu anahtar akışı arasında gerçekleştirilen XOR işlemi ile gerçek mesaj elde edilir. En son adımda ise CRC değeri hesaplanır ve daha

sonra mesajın bütünlüğü sağlanması için mesaja eklenen CRC değeri ile karşılaştırılır. [6]

3.3. TKIP

IEEE 802.11 kablosuz ağ sistemlerinin çoğunda donanım tarafından WEP desteklenmektedir. Donanım yapısını değiştirmeksizin WEP'in eksiklerini kapatabilmek amacıyla TGi tarafından Geçici Anahtar Bütünlük Protokolü diğer bir deyişle TKIP geliştirilmiştir. TKIP kısa vadeli bir çözüm olarak üretilmiştir ve donanım üzerinde sürücü veya yazılım güncellemesi ile kurulumu mümkündür. Bu ayarlanmış donanım üzerinde koşmanın getirdiği bazı kısıtlamalar şunlardır:

- Ayarlanmış sistemlerin yazılım veya aygıt yazılımlarının güncellenebilir olması
- Mevcut WEP donanım gerçeklemesinin değiştirilmeden kalması
- Yapılan düzeltmelerden kaynaklanan performans kaybının minimize edilmesi

TKIP, WEP protokolünün bilinen eksikleri ile mücadele edebilmek için uyarlanan algoritmalardan oluşan bir protokoldür. TKIP WEP'e dört yeni algoritma eklemektedir. Bunlar :

- Sahte mesaj korumasını sağlamak için Michael adı verilen bir kriptografik mesaj bütünlük kodu (MIC),
- Tekrarlama saldırılarını önlemek amacıyla yeni bir IV sıralama disiplini,
- Herkes tarafından bilinen IV değerlerinin zayfı anahtarlarla olan ilişkisini kaldırmak amacıyla bir paket özel anahtar üretme fonksiyonu,
- Aynı anahtar kullanımından kaynaklanan saldırıları önlemek amacıyla her adımda yeni şifreleme ve bütünlük anahtarları üreten anahtar yönetimi. [20]

3.3.1. Michael

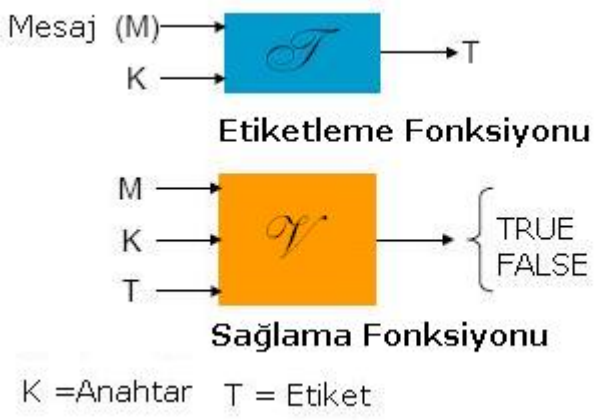
Bir MIC algoritması verinin anahtarlı fonksiyonunu gönderici de hesaplar ve sonuç değerini bir etiket şeklinde veri ile beraber alıcıya gönderir. Alıcı bu değeri tekrar hesaplar ve göndericinin kendisine gönderdiği etiket ile karşılaştırır. Eğer iki değer

aynıysa alıcı verinin güvenilir olduğunu düşünüp veriyi kabul eder, aksi takdirde verinin sahte olduğını düşünüp kabul etmez.

IPSec tarafından kullanılan HMAC-SHA ve genellikle finansal uygulamalarda kullanılan DES-CBC-MAC gibi mesaj bütünlük kodu hesaplama algoritmalarının mevcut WLAN donanımı üzerinde performansı düşürmeden hesaplanması çok zordur. [20]

Her MIC üç kısımdan oluşur:

1. Gizli doğrulama anahtarı K (sadece gönderici ve alıcı arasında paylaşılır)
2. Etiketleme Fonksiyonu (Tagging Function)
3. Sağlama Fonksiyonu (Verification Predicate)



Şekil 3.2 : Michael Mesaj Bütünlük Kodu Hesabı Blok Şeması

Etiketleme fonksiyonu M mesajını ve K anahtarını giriş olarak alır ve çıkış olarak mesaj bütünlük kodu adı verilen T etiketini üretir. M mesajı sahtecilikten, göndericinin T etiketini hesaplaması ve bunu M mesajıyle birlikte yollamasıyla ile korunur. Sahtecilik olup olmadığının tespiti için alıcı K, M ve T girişlerini sağlama fonksiyonuna alır. Eğer sağlama fonksiyonu TRUE değerini döndürürse, T etiketi etiketleme fonksiyonu tarafından üretilmesi gereken değere eşit demektir.Aksi durumda FALSE değeri döner. Eğer dönen değer FALSE ise mesajın sahte olduğu kabul edilir, diğer durumda mesaj güvenilir olarak kabul edilir (Şekil 3.2). Bir MIC değerinin güvenilir olarak kabul edilebilmesi için bir saldırganın daha önce hiç görmediği bir M mesajından, K anahtarını bilmeksizin, T etiketini elde edemiyor olması gerekir.

Michael, TKIP mesaj bütünlük kodunun özel adıdır. Niels Ferguson tarafından tamamen yeni bir yapıda tasarlanmıştır. Michael anahtarı 64 bittir ve iki 32 bit Endian kelimeleri (K_0, K_1) olarak temsil edilir. Michael etiketleme fonksiyonu ilk olarak mesajı 0x5a hex değeri ile doldurur ve toplam mesaj uzunluğunu 32 bitin katlarına getirecek şekilde mesaja sıfır(0) ekler. Daha sonra sonucu 32 bit boyutunda M_1, M_2, M_3,.....M_n kelime dizilerine bölümler.

Son olarak MIC değeri, anahtar değeri ile başlayarak ve b( ) blok fonksiyonunu her mesaj kelimesine yinelemeli olarak uygulanmasıyla hesaplanır. Bu işlemi gerçekleştiren işlemler aşağıdaki gibidir [32] :

Michael Etiketleme Fonksiyonu :

Giriş : (K_0, K_1) anahtarı ve M_0,...,M_N mesajı

Çıkış : MIC değeri (V_0, V_1)

MICHAEL ((K_0, K_1) , (M_0,...,M_N))

$(L,R) \leftarrow (K_0, K_1)$

for i=0 to N-1

$L \leftarrow L \oplus M_i$

$(L, R) \leftarrow \mathbf{b}(L, R)$

return (L,R)

Görüldüğü gibi döngü toplam mesaj kelimesi sayısı olan N defa dönmektedir. Sonuçta elde edilen iki kelime sekiz baytlık bir diziye dönüştürülür ve mesaja eklenir. Etiketleme fonksiyonunda kullanılan b( ) blok fonksiyonu, birbirini izleyen toplamalar ve XOR işlemlerinden oluşan Fiestel tipinde bir yapıya sahiptir.

Michael Blok Fonksiyonu (b) :

Giriş : (L,R)

Çıkış : (L,R)

*b(*L,R)

$R \leftarrow R \oplus (L <<< 17)$

$L \leftarrow (L + R) \bmod 2^{32}$

$R \leftarrow R \oplus XSWAP(L)$

$L \leftarrow (L + R) \bmod 2^{32}$

$R \leftarrow R \oplus (L <<< 3)$

$L \leftarrow (L + R) \bmod 2^{32}$

$R \leftarrow R \oplus (L >>> 2)$

$L \leftarrow (L + R) \bmod 2^{32}$

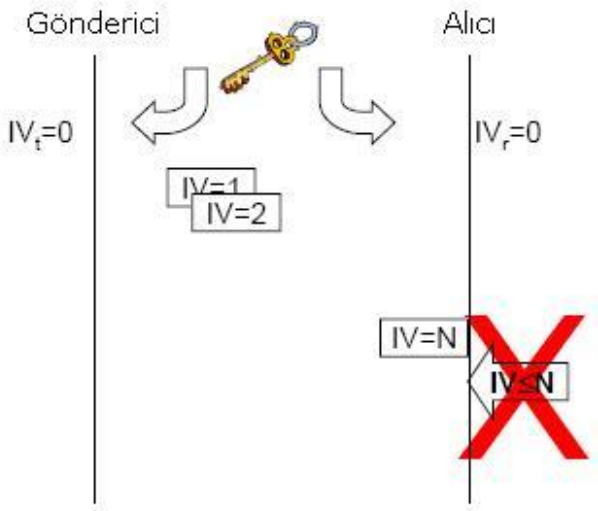
return (L,R)

Bu algoritmada <<< ifadesi 32 bit değerlerde sola döndürme operatörü olarak, >>> ifadesi de sağa döndürme operatörü olarak kullanılmıştır. XSWAP ifadesi bir kelimede düşük anlamlı iki baytın ve yüksek anlamlı iki baytın yer değiştirilmesi işlemini gerçekleştiren fonksiyon için kullanılmıştır. [33]

3.3.2. IV Sıralama Disiplini

MIC tarafından tespit edilemeyen saldırı tekrarlanmış paket saldırısıdır. Bu durum bir saldırganın iletimde olan bir geçerli paketin kaydını alıp onu tekrar iletmesidir. Bu problemle baş etmenin yolu MIC anahtarı ile beraber bir paket sıra numarasının da belirlenmesidir. MIC anahtarı değiştirildğinde bu sıralama kümesinin da yeniden başlatılması gerekir. Bu senaryoda iletim yapacak taraf, eğer sıra numarası kümesi tükenmişse eski MIC anahtarı tarafından korunan veriyi yollamaktan sakınmalıdır. Bu tükenme durumunda iletici tarafın seçenekleri a) tüm iletimi durdurmak, b)MIC anahtarını yenilemek, c) hiçbir kriptografik koruma olmadan sonradan ortaya çıkan yeni bir trafik oluşturmaktır. Bunlardan herhangi bir senaryo anahtarla korunan veriyi risk altına alır.

TKIP da bu klasik senaryoyla oldukça uyum sağlamaktadır. Tekrarları önlemek için WEP IV değerini paket sıra numarası olarak kullanır. Hem gönderici hem alıcı her yeni TKIP anahtarları üretildiğinde paket sıra numarası kümelerini sıfırlar. Gönderici gönderdiği her pakette bu değeri bir attırır. TKIP alıcı tarafında da, gelen paketlerin uygun IV sıralamasına uymasını gerektirir. TKIP bir paketin sıralamaya uygun olup olmadığına o paketin IV değerini aynı anahtarla şifrelenmiş ve daha önce güvenilir olduğu kabul edilmiş MPDU'nun IV değeri ile karşılaştırarak karar verir. Şekil 3.3'te görüldüğü gibi sıralamaya uygun olmayan bir MPDU olduğunda TKIP bunu bir tekrar olarak düşünür ve paketi düşürür.



Şekil 3.3 : IV Sıralama Disiplini

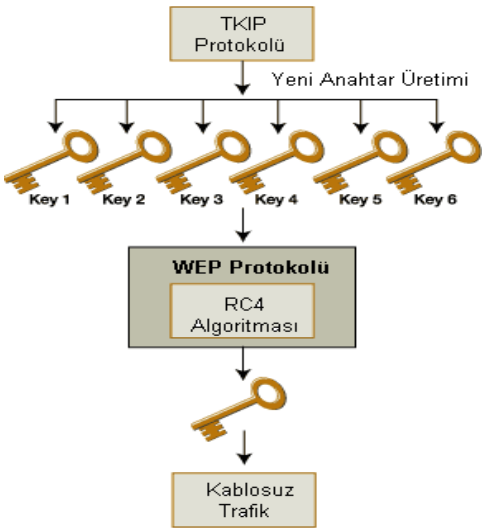
TKIP'ın geleneksel senaryodan ayrıldığı nokta, sıra numarasını MIC anahtarı ile değil TKIP şifreleme anahtarı ile ilişkilendirmesidir. Bunun sebebi WEP IV değerinin sıra numarası olarak seçilmesidir. Bu seçim ise mevcut WEP donanımının ve paket formatlarının kullanılabilmesi için yapılmıştır. IEE 802.11 standardı IV alanını paket parçaları (MPDU) ile ilişkilendirir. Ancak, erişim noktaları TKIP MIC değerini tüm paket üzerinden (MSDU) hesaplarlar. [33]

3.3.3. Farklı Anahtar Üretme

RC4 algoritmasınının yazarı olan Ron Rivest WEP'te bulunan anahtar planlama sisteminin çok zayıf olmasından dolayı bu duruma iki farklı çözüm önermiştir. Bunlardan ilki şifrelemeye başlamadan önce PRGA tarafından üretilen çıkışın ilk 256

baytının gözden çıkarılmasıdır. Diğeri ise anahtar planlama algoritmasının kuvvetlendirilmesidir. Bu kuvvetlendirme için de anahtar ve IV değerlerine birleştirilmeden önce MD5 gibi bir karıştırma fonksiyonunun uygulanması şeklindedir.

TKIP'ın sağladığı paket-başına anahtar (per-packet key - PPK) yapısı ise RC4'ün yanlış kullanımını düzeltmek için kullanılan bir özelliktir. Yeni pakete özel anahtar yapısı TKIP Anahtar Karıştırma Fonksiyonu (TKIP Key Mixing Function) olarak adlandırılır ve diğer karıştırma fonksiyonlarından daha basit bir yapıdadır. Bu fonksiyon giriş olarak temel anahtarı, göndericinin MAC adresini ve paket sıra numarasını alır ve her pakete özel yeni bir WEP anahtarı oluşturur. [20]



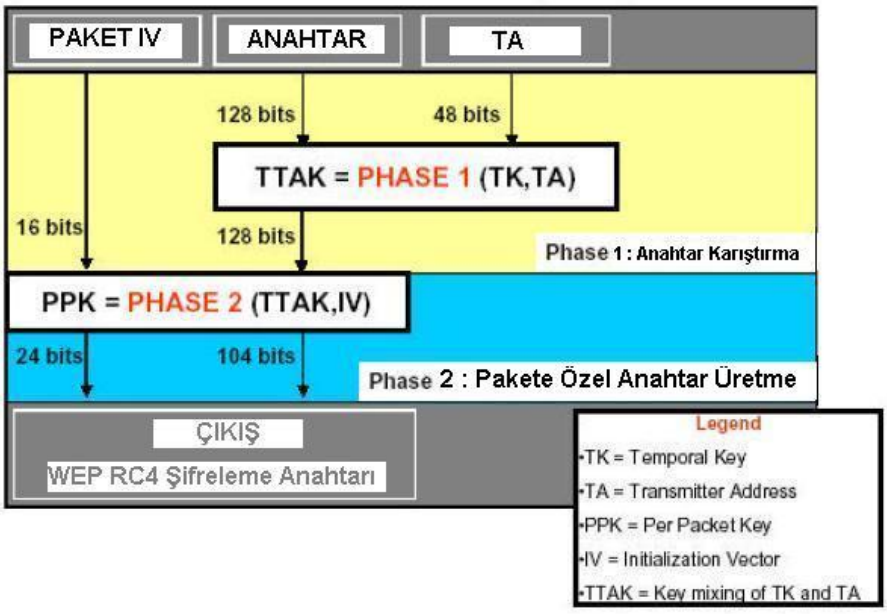
Şekil 3.4 : TKIP Farklı Anahtar Üretme Fonksiyonunun Kullanım Yeri

Bu yapının uygulanabilmesi için aşağıdaki koşulların sağlanması gerekmektedir :

- Şifreleyici ve deşifreleyici , WEP temel anahtarı yerine kullanılacak olan geçici anahtar (temporal key – TK) adı verilen 128 bit gizli anahtarı paylaşmalıdır.
- Şifreleyici ve deşifreliyicinin her ikiside RC4 algoritmasını kullanmalıdır.
- Hiçbir IV değerinin herbir TK ile birlikte birden fazla kullanılmadığından emin olunmalıdır. Burada IV değerinin, sıfır değeri ile başlayan 16 bitlik bir sayaç olarak yaratılması beklenir. Ayrıca tüm 16 bit IV kümesi tükenmeden TK değerinin değiştirilmesine dikkat etmelidir.

Anahtar Karıştırma fonksiyonu iki ana bölümden oluşur. Bu bölümlerin her birinde WEP'in yapısal kusurlarını telafi etmektedir. Birinci evre (phase 1) tüm iletim boyunca aynı anahtarın kullanımını engellemektedir. İkinci evre (phase 2) ise herkes tarafından bilinen IV değerinin paket anahtarları olan ilişkisini kaldırmaktadır. İki evreden oluşmasının nedeni WEP tabanlı cihazların yüksek işlem yapabilme kapasitesinden yoksun olması ve işlem sayısını en aza indirgenmek istenmesidir. [34]

Birinci evre geçici anahtarı ve göndericinin adresini (transmitter address - TA) kullanır. Bu evrede elde edilen ara anahtar ikinci evrede IV değeri ile beraber kullanılır ve pakete özel anahtar (PPK) üretilir. Her TK ile şifrelenen paket için IV değeri farklı olmalıdır.
İki evre aşağıda görülen şekille özetlenebilir:



Şekil 3.5 : TKIP Protokolünün Evreleri

3.3.3.1. Birinci Evre

Bu evrede göndericinin adresi ve geçici anahtar giriş olarak alınır ve bir ana anahtar üretilir. TK ve TA'nın her baytı yinelemeli olarak bir S-Box'a indeks oluşturmak için XOR işlemine tabi tutulur. S-Box'lar lineer olmayan yer değiştirme tablolarıdır. MAC adresinin geçici anahtar ile karıştırılması, farklı istasyonların ve erişim noktalarının, aynı geçici anahtarları kullanıyor olsalar bile farklı ara anahtarlar üretmesini sağlar. Bu yapıyla her istasyondaki pakete özel şifreleme anahtar akışlarının birbirinden farklı olması sağlanmış olur. Birinci evrede üretilen ara anahtar sadece geçici anahtar değeri

değiştiği zaman hesaplanmalıdır, bu yüzden çoğu sistem bu değeri performans optimizasyonu olarak saklar. Bu değer 2^{16} pakete kadar geçerli olacaktır.

3.3.3.2. İkinci Evre

Bu evrede paket sıra numarasını birinci evrede üretilen ara anahtara bağlı olarak şifrelemek için basit bir şifreleme kullanılır ve 128 bitlik pakete özel anahtar üretilir. İkinci evrede üretilen çıkışın ilk 2 baytı gerçekte WEP IV değerine, geriye kalan 13 bayt ise temel WEP anahtarına karşılık gelmektedir.

İkinci evrede kullanılan basit şifreleme yöntemi Fiestel yapısına sahiptir. Fiestel yapısında içindeki döngüde $(L,R) \rightarrow (R, L \oplus f(R))$ yapısına uygun dönüşümü gerçekleştirmektedir. Michael'a benzer şekilde bu şirelemede yukarıda bahsettiğimiz döngüdeki işlemler XOR, kaydırma, döndürme ve tablo tarama gibi basit işlemlerle gerçekleştirilir. Bu basit işlemler 802.11 cihazlarında genelde bulunan işlemci tipi için de fazla yük olmayan işlemlerdir. [34]

Bu evrede ayrıca paket sıra sayacının 8 en anlamlı bitini WEP IV'nin ilk iki baytına atar ve en düşük anlamlı bitlerini de IV'nin üçüncü baytına atar. Daha sonra IV'nin ikinci baytının en anlamlı 8 bitini maskeler. Bunu WEP'in anahar oluşturma süreclerinde bilinen zayıf bir RC4 anahtarını üretmesini engelleme için yapar.

3.3.4. Anahtar Yönetimi

TKIP algoritmaları iki farklı anahtarı gerektirmektedir. Bunlar farklı anahtar üretiminde kullanılan 128 bit anahtar ve Michael tarafından kullanılan 64 bit anahtardır. TKIP bu anahtarların her oturum ilişkilendirmesinde yeni olarak alındığını kabul eder. TGi bu amaca uygun olarak 802.1X protokolünü hem doğrulama hem de anahtar yönetimine uyarlamıştır. IEEE 802.1X ilişkilendirme işleminden sonra doğrulama işlemini gerçekleştirir, daha sonra yeni bir ana anahtar üretir ve son olarak arka arkaya kullanımı için bu anahtarı dağıtır. Daha sonra istasyonlar ve erişim noktaları TKIP tarafından ihtiyaç duyulan anahtar çiftlerini üretmek için bu ana anahtarı kullanır. [33]

3.4. CBC-CCMP

CBC-CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol) TKIP gibi WEP'in zayıflıklarına çözüm üretmek amacıyla tasarlanmıştır fakat mevcut donanım ile yumlu olmadığından dolayı uzun vadeli bir çözüm olarak görülmektedir. Bu sistemin WEP ve WPA'dan en büyük farkı şifreleme algoritması olarak AES [3] (Advanced Encryption Standart) kullanmasıdır. [20]

3.4.1. AES Algoritması

AES Kasım 2001 tarihinde Federal Government Encryption Standart haline gelmiştir. 1977 yılında benimsenen Data Encryption Standart (DES)'in yerini almak üzere tasarlanmıştır.

AES simetrik anahtarlı blok şifreleme algoritmasıdır. Şifreleme ve deşifreleme için aynı yani simetrik anahtar kullanır. AES 128, 192 ve 256 bit anahtarları desteklemektedir. Şifreleme doğru bir şekilde kullanıldığı takdirde daha uzun anahtar daha fazla güvence anlamına gelmektedir. Kriptograflar, ticari veya özel uygulamalarda 128 bit anahtarların uzun yıllar yeterli güvenliği sağlayacağını düşünmektedirler. Bu yüzden AES'in 196 ve 256 bit anahtar desteği günümüzde pratik olarak gerekliliğinden değil geleceğe yönelik olarak tasarlanmıştır.

Blok şifreleme sabit uzunluklu bir bayt katarı üzerinde çalışırken, RC4 gibi akış şifreleme algoritmaları belirli bir zamanda tek bir bayt üzerinde işlem yaparlar. Bir bolktaki toplam bit sayısına şifrelemenin blok boyutu (block size) adı verilir. AES 128 bit yani 16 bayt blok boyutunda çalışır. Blok şifreleme yapılacak veri bloğu, blok boyutunun katı değilse, şifrelemeden önce bir doldurma işlemi gerçekleştirilir.

Blok şifrelemede bir işlem modu (mode of operation) kullanılır. İşlem modu şifrelemenin nasıl yapılacağını belirten kurallar kümesidir. Bu kuralların dışına çıkılırsa blok şifrelemenin sağladığı güvenlik tehlikeye atılabilir. AES tarafından kullanılan bazı işlem modları Electronic Codebook (ECB), Counter Mode (CTR) ve Cipher-Block Chaining (CBC) şeklindedir.

3.4.2. İşlem Modları

3.4.2.1. Sayaç Modu (Counter Mode - CTR)

Bu modda yardımcı veri olarak monoton olarak artan bir sayaç kullanılır. Eğer M mesajını M_1, M_2,……..M_n olarak ifade edersek sayaç modunu şu şekilde ifade edebiliriz:

K anahtarı atandığında sayac←0 atanır

Her M = M_1, M_2,……..M_n mesajı için

başlangıç_sayacı ← sayaç

i=1 den n'e kadar

$C_i \leftarrow M_i \oplus E_K$ (sayaç) , sayaç ←sayac+1

sifrelenmis_mesaj = başlangıç_sayacı C_1, C_2, …..C_n

(E_K () → K anahtarı işe şifreleme işlemi)

Görüldüğü gibi sayaç modu sayacı şifreler ve sayaç değerini şifrelenen her blok için bir attırır. Daha sonra şifrelenen sayac değeri gerçek metin ile şifrelenerek şifrelenmiş metin oluşturulur. Başlangıc sayacı değeri şifrelenmiş metinin başına eklenir. Bunun amacı deşifre işlemi yapılacağı zaman sayacın nerede yeniden başlatılacağını haber vermektir.

Sayaç modu blok şifrelemeyi basit bir şekilde yaptığı için gerçekleştirilmesi çok zahmetli ve zor değildir. Ancak bu mod aynı anahtar değeri ile aynı sayacın kullanılması durumunda oldukça kötü bir şekilde başarısız olur. Bu yüzden her oturumda yeni anahtar sağlayan anahtar yönetimi olmadıkça sayaç modunun kullanımı güvenli değildir.

3.4.2.2. Şifre--Blok Zincirleme (Cipher-Block Chaining - CBC)

CBC en geniş çapta kullanılan blok şifreleme işlem modudur. CBC önemsiz bilgi kaçaklarını önlemek amacıyla rastgele seçilmiş bir başlangıç vektörü kullanır. Eğer M mesajını M_1, M_2,……..M_n olarak ifade edersek CBC modunu şu şekilde ifade edebiliriz:

Her M = M_1, M_2,……..M_n mesajı için

IV ← rastgele seçilmiş değer

başlangıç_IV ← IV

i=1 den n'e kadar

$C_i \leftarrow E_K (M_i \oplus IV)$, IV ←C_i

sifrelenmis_mesaj = başlangıç_IV C_1, C_2, …..C_n

CBC modu gerçek metin ile rastgele üretilmiş IV değeri arasında XOR işlemini gerçekleştirir.Daha sonra elde edilen metin üzerinde şifreleme işlemi gerçekleştirilir. Bu XOR ile oluşturulmuş değerin şifrelenmesiyle oluşan değer, bir sonraki adımda kullanılmak üzere IV'nin yeni değeri olarak atanır. Bir sonraki adımdaki şifreleme öncesi XOR işlemi bu yeni IV ile gerçekleştirilir. [35]

CBC modu bu işlemleri bir mesajda bulunan her veri bloğu için gerçekleştirir. IV her mesaj için rastgele olarak seçilir. Başlangıc IV değeri şifrelenmiş metinin başına eklenir. Bunun amacı deşifre işlemi yapılacağı zaman IV'nin nerede yeniden başlatılacağını haber vermektir. IV seçiminin rastgele olmaması durumunda CBC modu oldukça kötü bir şekilde başarısız olur. [20]

3.4.2.3. CCM

AES'in var olan modlarından hiçbiri 802.11i için gerekli olan özellikleri için yeterli ve uygun özelliklere sahip değildir. İstenilen özellikler şu şekildedir:

- Gizlilik ve bütünlük için tek bir anahtar kullanması, anahtar yönetiminin kattığı yükün azaltılması, AES içindeki anahtar planlamasında geçen hesaplama zamanını minimize etmek.
- Veri kısmı kadar gerçek metin halindeki paket başlığı için de bütünlük kontrolü sağlamak.
- Gecikmeyi azaltmak amacıyla ön hesaplamalara izin vermek. Paketler kaybolabilir ve alıcı hiçbir zaman hedefe varamayacak paketleri için ön hesaplama yapabilir. Alıcıdaki işlemler nadiren de olsa gözden çıkarılır.

- Sistemdeki yararlı yükü arttırmak için eşgüdümlü işlemeyi (pipelining) desteklemek.
- Maliyeti uygun seviyede tutmak için basit ve küçük geçekleme boyutu.
- Her paket için küçük ek yük.
- Patent hakları yüzünden zorluk çıkarabilecek modlardan kaçınmak.

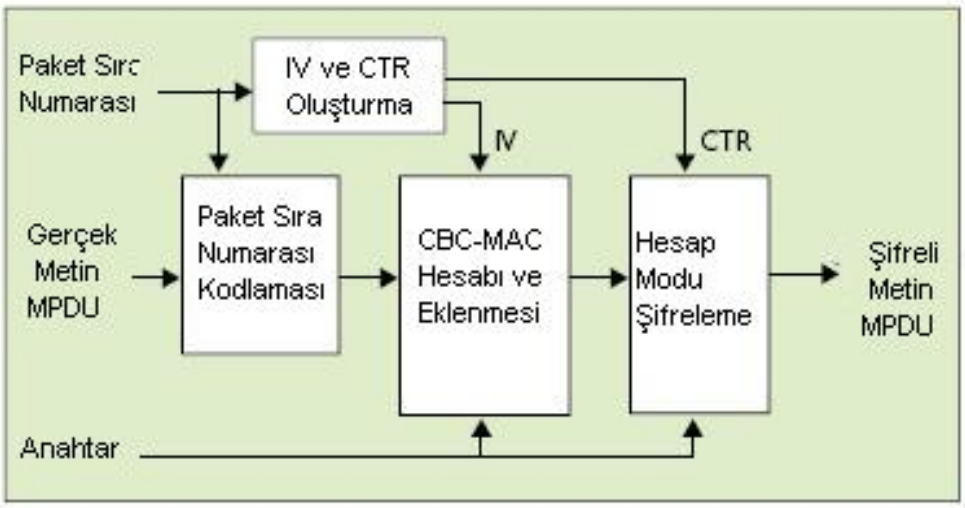
Tüm bu koşullara uyum sağlayabilmesi amacıyla CCM adı verilen yeni bir mod geliştirilmiştir.

CCM çok iyi bilinen ve geniş çapta uygulanan iki tekniği bir araya getirir. Şifreleme için sayaç modunu ve bütünlük kontrolü için Cipher Block Chaining Message Authentication Code (CBC-MAC) kullanır. Her iki algoritma da hem alıcı hem gönderici tarafında temel şifreleme işlemleri gerçekleştirilir. CCM Federal Information Processing Standart olarak kabul edilmesi için NIST'e yollanmıştır.

CCM hem gizlilik hem de bütünlük için aynı anahtarı kullanır. Bu normal şartlarda tehlikeli olabilecek bir durumdur. Ancak CCM bu kullanımdan doğabilecek sorunları önlemek amacıyla CBC-MAC tarafından kullanılan başlangıç vektörü uzayı ile sayaç modu tarafından kullanılan uzayın birbiri ile hiçbir zaman kesişmemesini garanti eder. CCM'nin altında yatan bu varsayımda, eğer AES bir sahte ve rasgele permütasyon olarak davranırsa, her iki uzaydaki şifreleme işleminin çıkışları birbirinden bağımsız olacaktır. [20]

3.4.3. CCMP Protokolü

CCM modunu kullanan bu protokol TKIP ile birçok noktada benzerlik gösterir. Varolan donanımın yol açtığı kısıtlamalardan bağımsızlığı TKIP'a göre daha düzenli bir çözüm sağlamaktadır. Aşağıdaki şekilde tek bir MPDU için CCM protokolünün kullanımını göstermektedir.



Şekil 3.6 : CCMP Protokolü

TKIP'a benzer şekilde CCMP de 48 bit IV kullanır. AES anahtarının ömrünü herhangi bir olası ilişkilendirmeden daha uzun olacağını garanti eder. Bu durumda anahtar yönetimi ilişkilendirme sürecinin başlangıcına sınırlandırılır ve anahtarın ömrü boyunca göz ardı edilir. CCMP yine TKIP'a benzer şekilde 48 bit IV değerini tekrarlama saldırılarını önlemek amacıyla sıra numarası olarak kullanır.

AES, TKIP ve WEP tarafından kullanılan RC4 şifreleme algoritmasından oldukça farklı olan özellikleri ile ayrılır. AES paket özel anahtar ihtiyacı sorununu ortadan kaldırmıştır yani bir pakete özel anahtar türetme fonksiyonu yoktur. Daha önce de bahsettiğimiz gibi AES bir oturumdaki tüm paketler için gizlilik ve bütünlük kontrolünde aynı anahtarı (ve ilişkilendirilmiş AES anahtar yönetimi) kullanır.

CCM MIC uzunluğu 2 bayt ve 16 bayt arasında değişebilir. CCMP ise 8 baytlık bir MIC kullanır ve bu yöntem belirgin bir şekilde Michael'dan daha güçlüdür. TKIP ve WEP'ten farklı olarak şifrelenmiş ICV değerine de ihtiyaç yoktur.
TKIP bütünlük koruma mekanizmasını tüm MSDU üzerinde, gizliliği ise MPDU üzerinde sağladığı için uygulama karmaşıklığı getirmektedir. BU iki işlemi CCM aynı anda gerçekleştirdiği için, gizlilik ve bütünlük koruma mekanizmalarının da aynı veri yapısına uygulanması gerekmektedir. CCMP aynı zamanda parçalama (fragmentation) saldırılarına karşı koruyabilmek için neredeyse paketin tamamını korumak zorundadır. [20][35]

3.5. SİMÜLASYON

IEEE 802.11 WLAN sistemleri için günümüzde mevcut olan güvenlik mekanizmalarının incelendiği bu tez çalışmasında, ilgili mekanizmaların karşılaştırması hazırlanan bir simülasyon yardımıyla yapılmıştır. Bu simülasyonda IEEE'nin kablosuz ağlar için geliştirdiği standartlardan 802.11b, 802.11g ve 802.11i, yani bu standartların fiziksel katman özellikleri ele alınmıştır. Daha sonra bu yapıya WLAN sistemleri için geliştirilmiş güvenlik mekanizmaları WEP, WPA ve WPA2 de eklenmiştir.

Bu simülasyon çalışmasında fiziksel katman ve güvenlik mekanizmalarını içeren kaynak kodlar Microsoft Visual C++ 6.0 ortamında MFC Dinamik Bağlantı Kütüphanesi (DLL) projesi olarak yazılmıştır. Gerekli kondifürasyonların kullanıcı tarafından kolaylıkla yapılmasını sağlayan arayüz ise Microsoft Visual Basic 6.0 ortamında tasarlanmıştır.

3.5.1. Fiziksel Katman

Simülasyonda gerçeklenen IEEE standartalarından ilki şu anda en geniş çaplı kullanılan ve WLAN sistemleri deyince ilk akla gelen standart olan 802.11b standartıdır. Bu standart için IEEE spesifikasyonunda belirtilen olası veri hizları 1, 2, 5.5 ve 11 Mbps şeklindedir.

Bir diğer standart 802.11g standardıdır. Bu standart için IEEE spesifikasyonunda belirtilen olası veri hizları 6, 9, 12, 18, 24, 36, 48 ve 54 Mbps şeklindedir.

Fiziksel katman kısmında yer verilen 802.11i standartının fiziksel katman özelliklerini 802.11g ile aynıdır.

MAC katmanı konfigürasyonunda ise erişim mekanizmalarına yer verilmiştir. Temel erişim metodu, RTS/CTS koruma mekanizmalı veya 802.11g spesifikasyonunda tanımlanan CTS-to-Self koruma mekanizması ile çalışılması mümkündür. Bu tez çalışmasında temel erişim metodu kullanılmıştır.

3.5.2. Güvenlik Mekanizmaları

Bu tez çalışmasının asıl hedefi farklı standartlar ve veri hızları kullanan ağlar üzerinde kablosuz ağlar için günümüze kadar geliştirilmiş güvenlik protokollerinin performansını ölçmektir. Proje içinde uygulanan mekanizmaları düşünürsek aşağıdaki seçenekler ile bu simülasyonun çalıştırılması mümkündür:

802.11b ağlar için :

1. Güvenliksiz
2. 40 bit Anahtarlı WEP
3. 104 bit Anahtarlı WEP
4. WPA

802.11g ağlar için:

1. Güvenliksiz
2. 40 bit Anahtarlı WEP
3. 104 bit Anahtarlı WEP
4. WPA (TKIP+Michael)
5. WPA2 (CBC-CCMP)

Simülasyonun "Güvenliksiz" seçeneği ile çalıştırılması tüm fiziksel katman ve veri hızı seçenekleri için mümkündür. Bu durumda hiçbir güvenlik mekanizması fonksiyonu çalıştırılmadan simülasyon gerçekleştirilecektir. Güvenlik mekanizmalarına sahip konfigürasyonlarda güvenlik seçeneğinin ağ performansını nasıl etkilediğini görebilmek için bu seçenekten elde edilen veriler önemlidir.

"40 bit ve 104 bit anahtarlı WEP" seçeneği 802.11b ve 802.11g ağların her ikisi için kullanılabilir. WLAN sistemleri için geliştirilmiş ilk güvenlik mekanizması olan WEP, 802.11b ve 802.11g ağlarda temel ve varsayılan olarak gelen güvenlik seçeneğidir.

WPA2 güvenlik mekanizması fiziksel katmanda 802.11i seçeneği seçildiğinde aktif duruma gelir ve 802.11g ağlarla aynı özellikleri gösteren fakat AES tabanlı CBC-CCMP protokolünü kullanan bir sistem olarak çalışır.

3.5.3. Giriş Parametreleri

Simülasyonun çalıştırılması aşamasında tasarlanan arayüzden kullanıcı tarafından seçilmesi veya belirlenmesi gereken parametreler mevcuttur. Bu parametreleri şu şekilde sıralayabiliriz:

- Simulation Time : Simülasyonun kendi içinde çalışacağı toplam birim zamandır. Fiziksel katman parametreleri de kullanılarak hesaplanan "slot" değeri ile simülasyonun gerçekleştirilmesinde kullanılan değerdir.Simulasyonun harcadığı gerçek zaman değeri bu değerden farklı olacaktır.
- Access Mechanism : Temel Erişim, RTS/CTS ve CTS-to-Self erişim mekanizmasından biri seçilir. CTS-to-Self sadece 802.11g ağlar tarafından desteklenmektedir. RTS/CTS mekanizması seçildiğinde RTS Eşik değerinin de belirlenmesi gerekir.Bu eşik değerinden büyük olan paketlerde koruma mekanizması devreye girecektir. Eğer her zaman koruma mekanizmasının çalışması isteniyorsa eşik değeri 0 olarak belirlenir.
- Physical Layer Configuration : Simüle edilmesi istenen WLAN için fiziksel katman belirlenir.
- Data Rate Configuration: Seçilen fiziksel katmanın desteklediği veri hızları arasından biri seçilir.
- Number of Nodes: Performans incelemesi sırasında etkili olan bir parametredir. Ağdaki toplam düğüm sayısı belirlenir.
- Packet Length Distribution: Üretilecek paketlerin uzunluklarını belirlemek üzere kullanılacak dağılım seçilir. Constant, Uniform veya Exponential dağılımlarından biri seçilebilir.
- Packet Length Mean : Üretilecek paket uzunluğu için ortalama değer belirlenir ve seçilen dağılımda kullanılır. İzin verilen maksimum değer 32768 bittir.
- Packet Generation Rate Configuration : Paket üretim oranını belirlemek üzere kullanılacak dağılım seçilir.
- Packet Generation Rate Mean: Saniyede üretilecek paket sayısının ortalaması belirlenir ve seçilen dağılım tarafından kullanılır.
- Security : Güvenlik mekanizmaları ile ilgili ayarlamaların yapıldığı bölümdür. Güvenliksiz bir ağ konfigürasyonu için "No Security" seçeneği işaretlenir. WEP

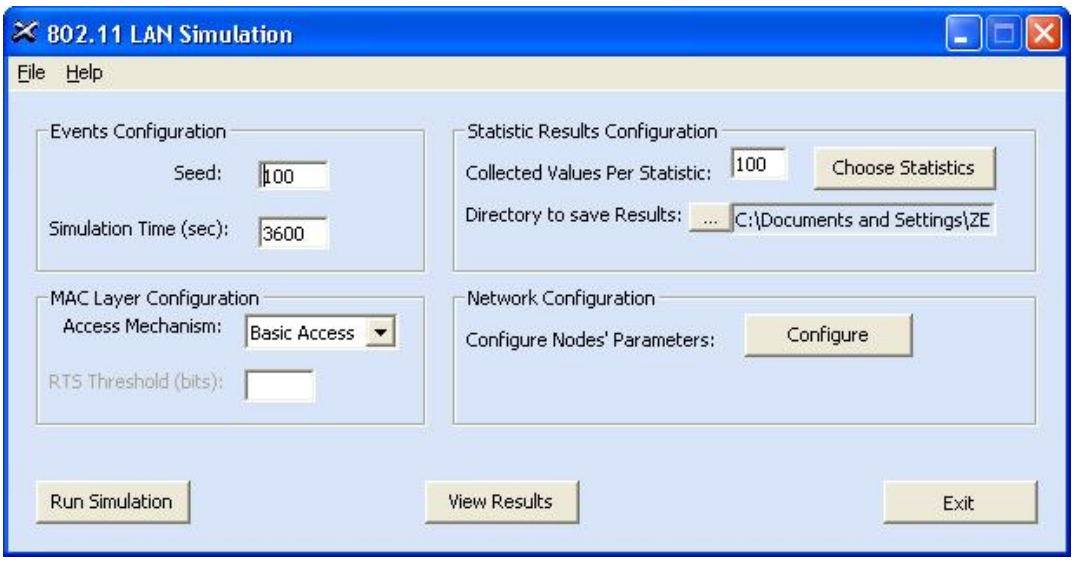
seçildiğinde , bu algoritmada kullanılacak anahtar uzunluğu da seçilir. WPA ve WPA2 seçeneklerinde ayrıca bir parametre seçimine gerek yoktur.

3.5.4. Sonuç Değerleri

Bu çalışmada yapılan değerlendirmelerde kullanılan en önemli sonuç değeri simülasyonun toplam işlem zamanıdır. Ayrıca simülasyon boyunca başarıyla üretilen toplam paket sayısını ve buna bağlı olarak toplam paket uzunluğu değerlerini elde ederiz. Bu iki değer kullanılarak da sistemdeki toplam yararlı yük, paket/sn ve kbits/sn cinsinden elde edilebilir.

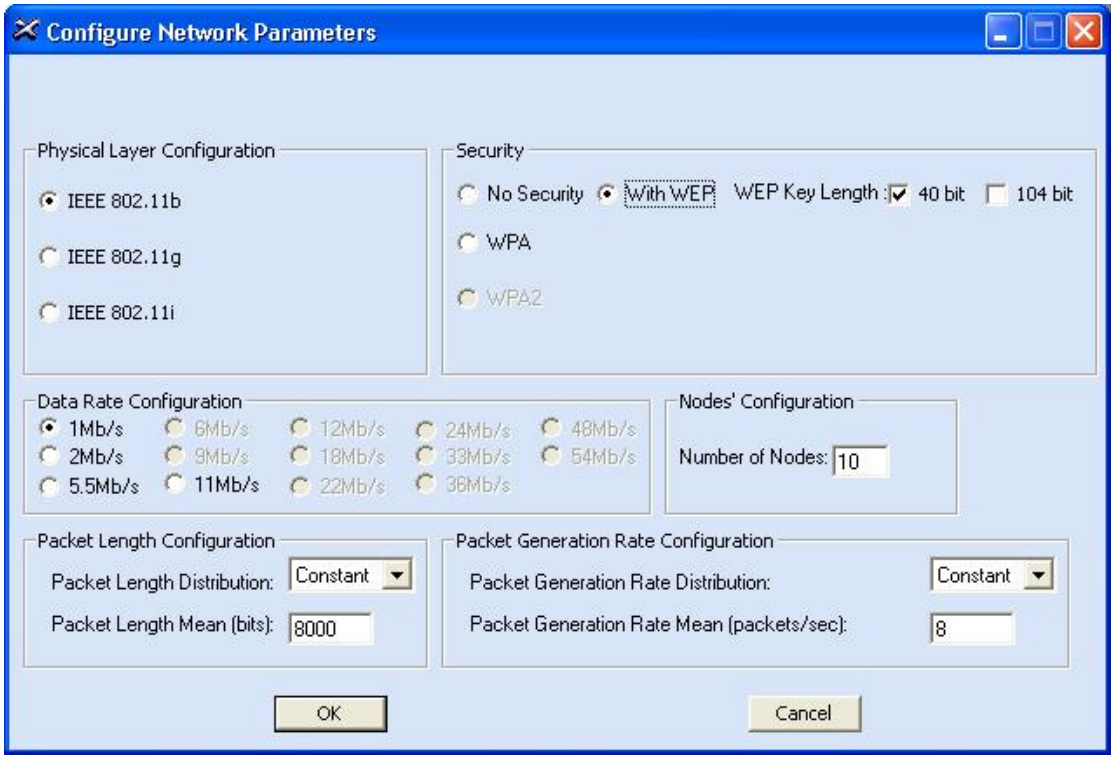
3.5.5. Arayüz

Simülasyon çalışmasının 4 ana arayüzü vardır. Bunlardan ilki giriş parametrelerinde bahsettiğimiz ilk üç parametrenin belirleneceği ana ekrandır.



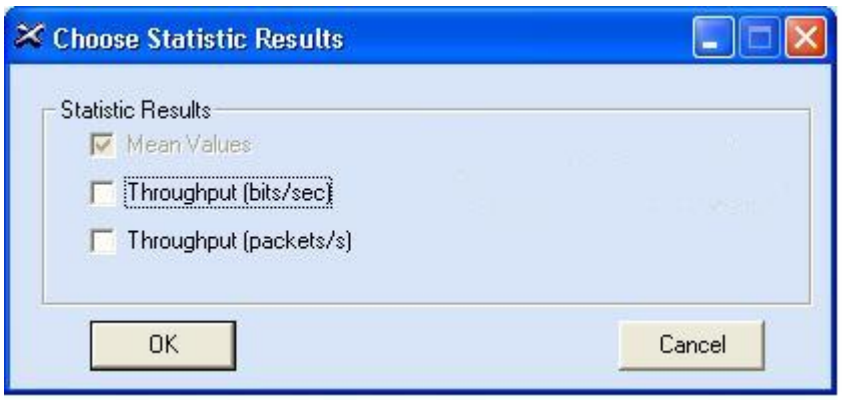
Şekil 3.7 : Simülasyon Programının Ana Ekranı

İkinci ekranımız ana ekrandaki "Configure" butonu ile eriştiğimiz ve ağ parametrelerinin belirlendiği ekrandır. Giriş parametreleri kısmında belirtilen parametrelerden ilk üçü hariç diğeleri bu ekranda belirlenir.



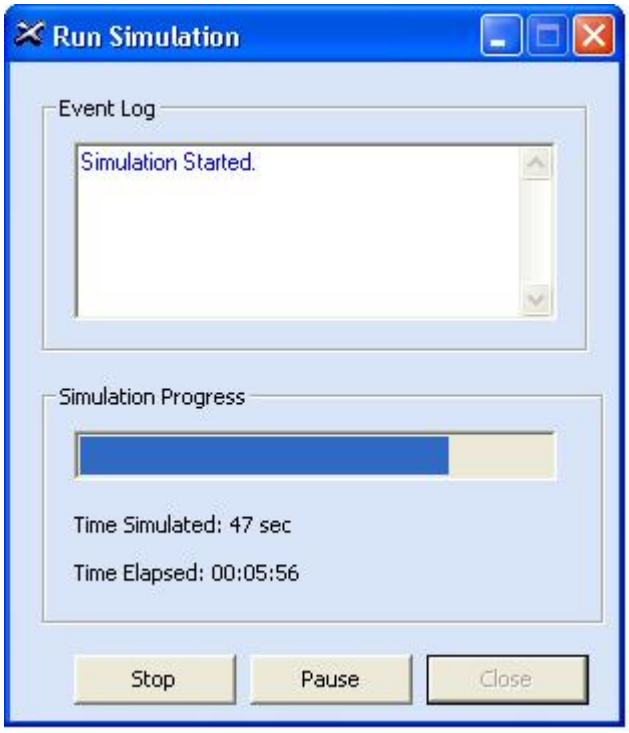
Şekil 3.8 : Simülasyonun Ağ Parametreleri Konfigürasyonu Ekranı

Üçüncü ekranımız ana ekranımızdan "Choose Statistics" butonu ile eriştiğimiz ve çıkış olarak almak istediğimiz parametrelerin belirlendiği ekrandır. Burada belirlenen değerler ana ekranda sonuçları kaydetmek için belirlediğimiz klasör içine metin dosyaları halinde kaydedilir.



Şekil 3.9 : Simülasyonun İstatistik Seçimi Ekranı

Dördüncü ekranımız ise simülasyon çalışırken gördüğümüz ekrandır. Burada ana ekranda belirlediğimiz simülasyon zamanı toplam geçen zaman takip edilebilir.



Şekil 3.10 : Simülasyonun Çalışma Anı Ekranı

3.6. DENEYSEL ÇALIŞMA

3.6.1.Amaç

802.11 ağların performansını inceleyen çalışmamızın bu bölümünde 802.11g kablosuz ağ standardının performansını birden çok istemci ile kurduğumuz bir ağ üzerinde inceleyen deneysel çalışmalar yapılmış, ağ trafiği ve belirlediğimiz güvenlik mekanizmalarının uygulaması yapılmıştır.

Bu deneysel çalışmayla aşağıdaki sorulara cevap aranmıştır :

- Farklı güvenlik mekanizmaları birden fazla istemci ile kurulmuş olan bir ağda sistem performansını (gecikme (delay), yararlı yük miktarı (throughput) gibi) nasıl etkiliyor?
- Farklı güvenlik mekanizmalarının varlığında farklı uzunluktaki paket sayısı kablosuz ağdaki performansı nasıl etkiliyor?
- Farklı güvenlik mekanizmalarının farklı trafik tiplerine göre güvenilirlikleri nasıl değişiyor?
- Tek istemci ile birden fazla istemcinin oluşturduğu ağlarda sistem performansı nasıl etkiliyor?

3.6.2. Metodoloji

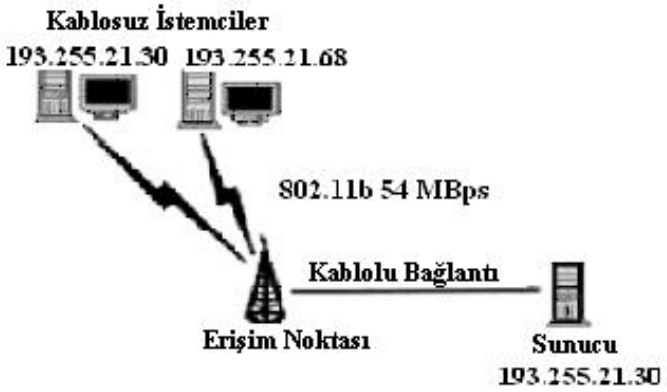
Çalışmanın tamamlanması için yapılması gereken 5 önemli aşama bulunmaktadır :

- Fiziksel ağ ortamının oluşturulması
- Güvenlik katmanlarının belirlenmesi ve konfigürasyonu
- Ağ trafiğinin oluşturulması
- Elde edilen sonuçların toplanması
- Elde edilen sonuçların değerlendirilmesi ve yorumlanması

3.6.2.1. Fiziksel Ağ Ortamının Oluşturulması

Laboratuar ortamında küçük boyutta bir kablosuz ağ oluşturulmuştur. Bu oluşturduğumuz kablosuz ağ aşağıda belirtilen elemanlardan meydana gelmektedir :

1 Adet Sunucu Bilgisayar : (Windows 2000 Advanced Server, 1.2 GHz, 256 MB RAM, Linksys AP yazılımı)
2 Adet İstemci Bilgisayar : (Windows XP Professional, 1.2 GHz, 256 MB RAM, Linksys Wireless PCI Card 802.11g 54mbps)
1 Adet Erişim Noktası : (Linksys Wireless Access Point 802.11g)



Şekil 3.11 : Deneysel Çalışmada Kullanılan Ağ Konfigürasyonu

Şekil 3.11'de gösterilen konfigürasyonda AP ve istemciler arasında iletişim hızı 54 Mbps, AP ve sunucu arasında 100 Mbps Ethernet bağlantısı mevcuttur.

3.6.2.2. Güvenlik katmanlarının belirlenmesi ve konfigürasyonu

Güvenlik katmanlarını belirlerken alınan ölçüt WEP doğrulama ve şifreleme algoritması ile beraber IEEE 802.1X doğrulama protokolüdür. Bu iki sistem kullanılarak 6 güvenlik katmanı yaklaşımı belirlenmiştir. Bu katmanlar şu şekildedir :

1. Güvenlik Katmanı Yok (No security) : Hiçbir güvenlik mekanizmasının olmaması üretici firmalar tarafından varsayılan olarak başlangıçta belirlenen ayardır.
2. 64-bit WEP Şifrelemesi ve WEP Doğrulaması : Bu katmanda geleneksel güvenlik mekanizması olan 64 bit WEP şifrelemesi ve WEP'in sağladığı doğrulama mekanizması kullanılmıştır.
3. 128-bit WEP Şifrelemesi ve WEP Doğrulaması : Bu katmanda 128 bit WEP şifrelemesi ve WEP'in sağladığı doğrulama mekanizması kullanılmıştır.
4. EAP-TLS Doğrulaması: IEEE 802.1X tarafından kullanıcıyı doğrulamak için dijital sertifika kullanan PKI-tabanlı doğrulama metodudur.

5. 64-bit WEP Şifrelemesi ile EAP-TLS Doğrulaması: 64 bit WEP şifrelemesi ile beraber EAP-TLS doğrulaması kullanılır.
6. 128-bit WEP Şifrelemesi ile EAP-TLS Doğrulaması: 128 bit WEP şifrelemesi ile beraber EAP-TLS doğrulaması kullanılır.

Bu katmanlardan ilk üç güvenlik katmanı IEEE 802.11 standardı ile desteklenen güvenlik mekanizmaları, 4-6 arasındaki akatmanlar ise IEEE 802.1X protokolünün sağladığı güvenlik mekanizmalarıdır.

3.6.2.3. Ağ Trafiğinin oluşturulması

Gerçekleştireceğimiz deneylerde tıkalı (congested) ve tıkalı olmayan (uncongested) ağlarda yapılmıştır. Bu sebeple kullanılan trafik üretecinin bu şartları yerine getirebilmesi gerekmektedir.

Trafik üretimi için gerekli olan sistemin seçiminde ölçüt olarak aldığımız kriterler şunlardır:

- Kablosuz ağlar için uygun olmalıdır
- 802.11g standardı ile uygun olmalıdır.
- Kullanıcıya paket boyutunun değişimine olanak sağlamalıdır.
- Trafik oluşturma algoritmasını kullanıcı seçebilmelidir.

3.6.2.4. Deney Sonuçlarının Toplanması

Uygun trafik üretecinin seçiminden sonra gerçekleştirilen deneylerin sonucunda ölçümlerin yapılabilmesi ve yorumlanması için elde edilen sonuçların toplanması gerekmektedir. Bu amaçla sunucu tarafında bilgileri toplamak için bir ağ analiz yazılımı kullanılmıştır ve bu yazılım ile istatistikler elde edilmiştir.

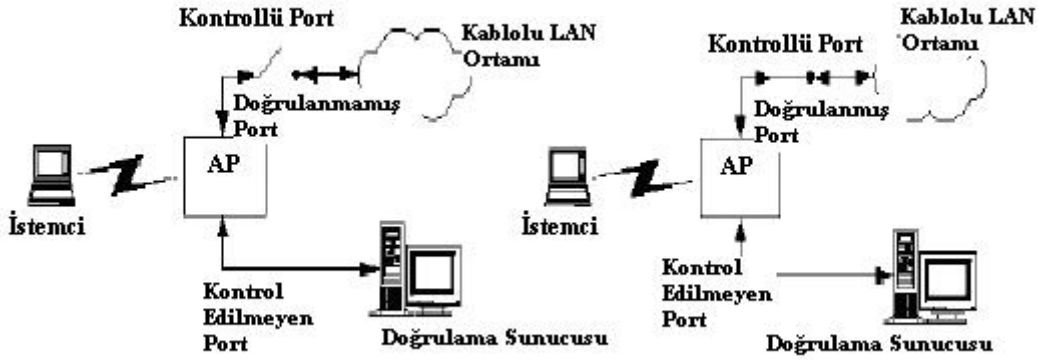
3.6.2.5. Elde Edilen Sonuçların Değerlendirilmesi ve Yorumlanması

Toplanan deney sonuçlarının değerlendirilmesi ve başta hedeflediğimiz performans ölçümü amacımıza uygun olarak değerlendirilmesi gerekmektedir. Gerek ağ analizini yaptığımuz yazılım ile gerekse topladığımız verileri değerlendirilen istatistiksel sonuçlar elde edilmiştir.

3.6.3. 802.1X Modeli Kurulumu

802.1X modelinde 3 önemli rol vardır :

- Doğrulayıcı :Doğrulama işlemlerini yapan ve ağ içindeki trafiği uygun şekilde yönlendiren porttur.
- Sağlayıcı :(802.11'deki client gibi) : Ağa ulaşmaya çalışan porttur.
- Doğrulama Sunucusu : Gerçek doğrulama işlemlerini gerçekleştiren bölümdür. En yaygın olan doğrulama sunucusu, uzaktan erişen kullanıcıları da doğrulayabilen RADIUS'tur. Şekil 3.12 kontrollü / kontrollü olmayan port kavramını göstermektedir. Şeklin ilk ve ikinci kısmında istemcinin doğrulamadan önceki ve sonraki durumu gösterilmiştir.



Şekil 3.12 : Kontrollü ve Kontrolsüz Port Kavramı

Kontrollü / kontrolsüz ifadeleri portları lojik olarak ifade eder. Aslında iki durumda da ağa aynı fiziksel bağlantı ile bağlanılır.AP tarafından yönlendirilen paketlerin hangi porttan gideceği istemcinin doğrulanmışlık durumuna göre belli olur. Doğrulama sunucusunun ilk doğrulama yaptığı durumda istemci sadece AP ile bağlantı kurar. Sonra istemci isterse ağın diğer kaynaklarına da erişebilir. Şunun altını çizmek gerekir ki doğrulama işlemi mutual (çift taraflı) gerçekleşir. Ağ ve istemci birbirlerini ayrı ayrı doğrular.

802.1X kullanılan WLAN'larda 2 çeşit anahtar oluşturulur:

- Oturum Anahtarları (Session keys-Pairwise keys) : Bağımsız bir istemci ile AP arasındadır ve bunlar arasında sanal bir port oluşturur.
- Grup Anahtarları (Groupwise keys): Aynı AP'ye bağlı istemciler tarafından paylaşılır.

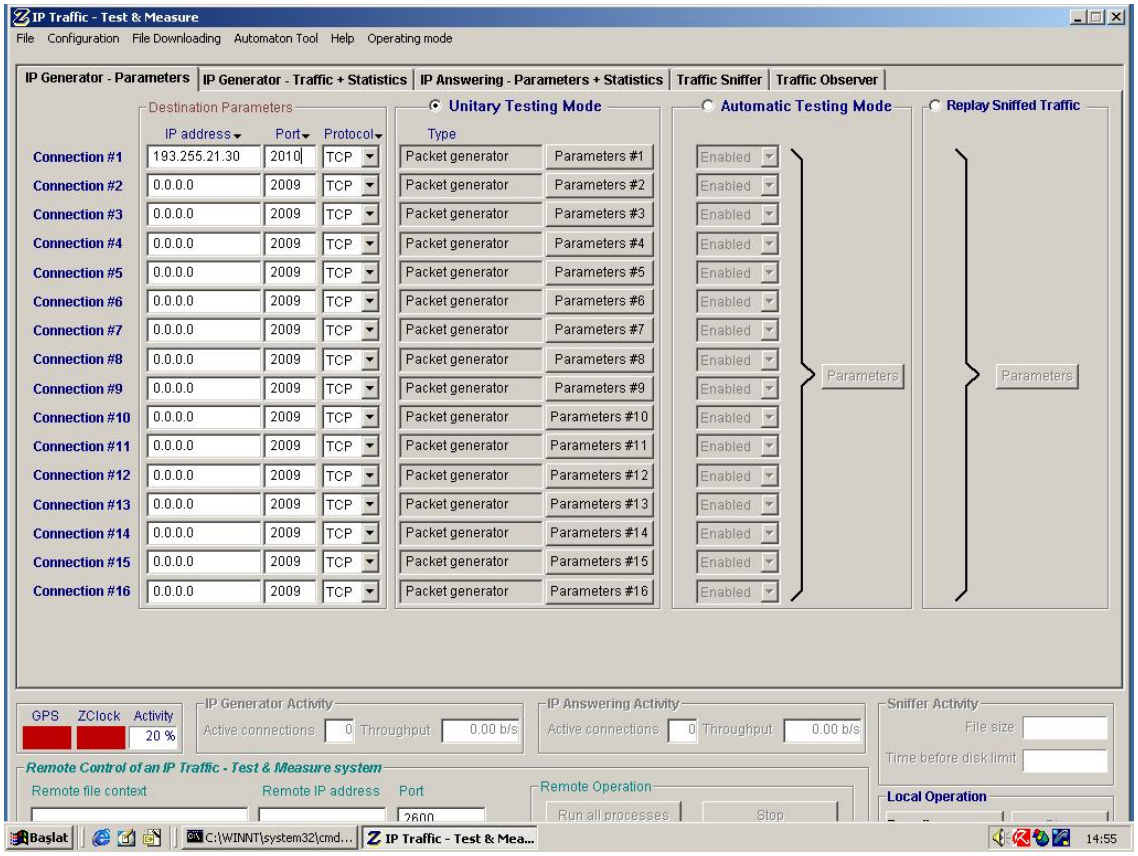
802.1X protokolünün WLAN sistemlerine güvenlik açısından getirileri vardır. 802.1X'in WEP standardına getirdiği ek özellikler şunlardır :

- Merkezi bir güvenlik yönetim modeli sunar.
- Doğrulama Sunucusu kullanıldığında şifreleme anahtarları dinamik olarak üretilir,bu da güvenliği arttırıcı bir özelliktir.
- Üst katmanların güçlü bir doğrulama mekanizmasına sahip olmasına yardım eder.

Daha önce belirtilen 4-6 arası maddelerdeki güvenlik katmanlarını oluşturabilmek için LucidLink RADIUS Server kullanılmıştır. RADIUS Sunucusu ve güvenlik sertifikaları ağ yapısında 802.1X doğrulama yapısını oluştururlar.

3.6.4. Trafik Üretimi

Deneyin en önemli aşamalarından biri trafik üretme aşamasıdır. Üretilmek istenen trafiğin ve bunu gerçekleştiren yazılımın hangi kriterleri sağlaması gerektiği bölüm 3.6.2.3 de belirtilmiştir.
Yapılan araştırmalardan sonra IP Traffic adlı yazılımın kullanılmasına karar verilmiştir. Bu yazılım kablolu ve kablosuz IP ağlarda ve Windows platformunda çalışabilen yapıdadır. Trafik üretme, yakalama, IP trafiğini tekrarlama, baştan sona performansı ölçme gibi işlemleri gerçekleştirebilmektedir. Ayrıca birden fazla bağlantının da kurulumuna izin veren bir yapısı vardır.



Şekil 3.13 : İstemci tarafında IP Traffic Programının Kullanımı

IP Traffic yazılımıyla oluşturulan gerçek zamanlı trafik Ethereal yazılımı ile yakalayarak analiz edilmiştir..Ethereal programı ile ilgili gerekli bilgiler Ek B'de verilmiştir. Bundan sonraki bölümlerde deneyde kullanılan parametrelerin ve de programların ayarlanışını incelenmiştir.

3.6.4.1. Trafik Üretiminde Kullanılan Parametreler

- Toplam Paket Sayısı

IP Traffic programı 0 ile 60000 arasında değişen sayıda paket üretimine izin vermektedir. Bu değer aralığından 43000 değerini rastgele bir değer olarak kullanılmıştır.

- Bant Genişliği

802.11g 'yi destekleyen bir AP kullanılmasından dolayı istemcilerde üretilen trafiğin bant genişliği teorik olarak ve standartlara göre maksimum 54 Mbps'dır. Fakat sistemin tıkalı olduğu durumlarda nasıl davranacağının da incelenebilmesi için istemcilerin ürettiği trafiğin bant genişliği 55 Mbps olarak ayarlanmıştır.

Yapılan tüm testlerde farklı yoğunluk durumuna sahip ağ tiplerini inceleyebilmek amacıyla bant genişlikleri 2000-25000-55000 kb/s olarak ayarlanmış ve bu değerler için ayrı ayrı tüm testler gerçekleştirilmiştir.

- Trafik Tipi

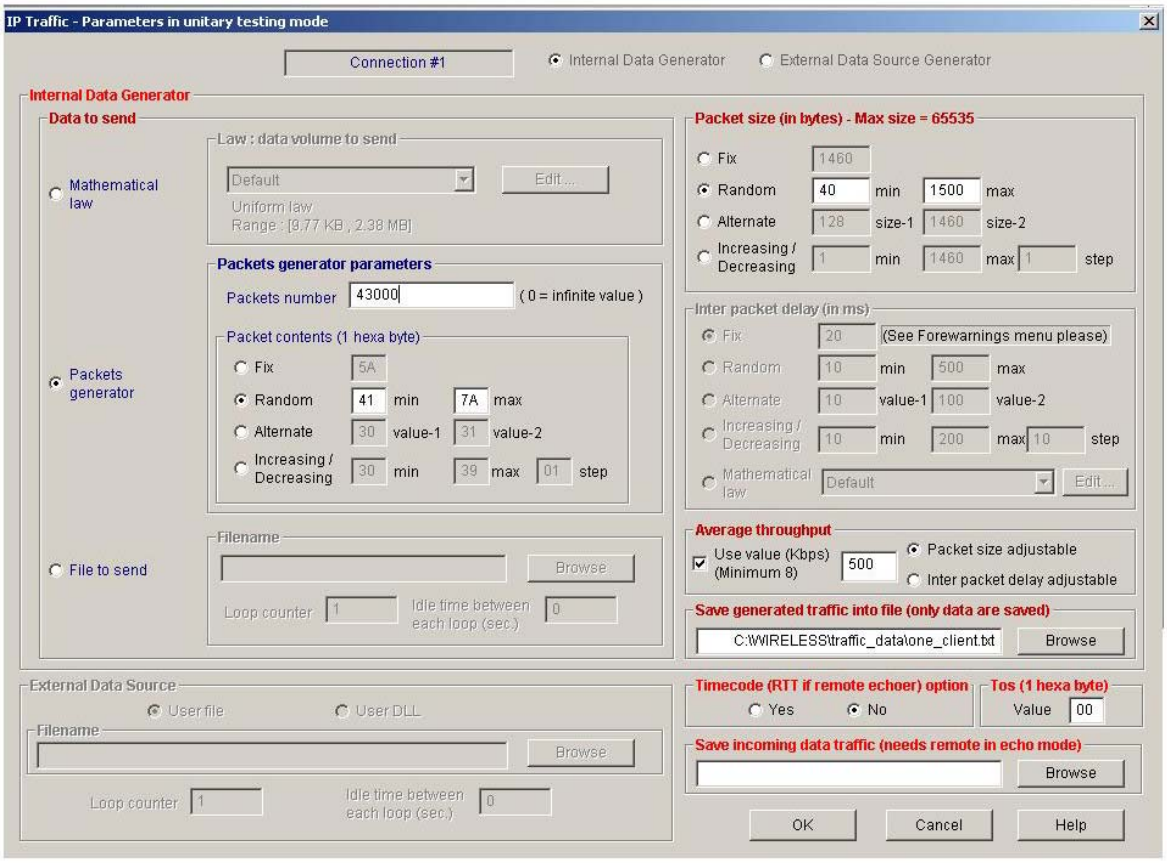
Deney çalışmasında TCP ve UDP protokollerine göre trafik üretimi gerçekleştirilmiştir.

- Paket içerikleri

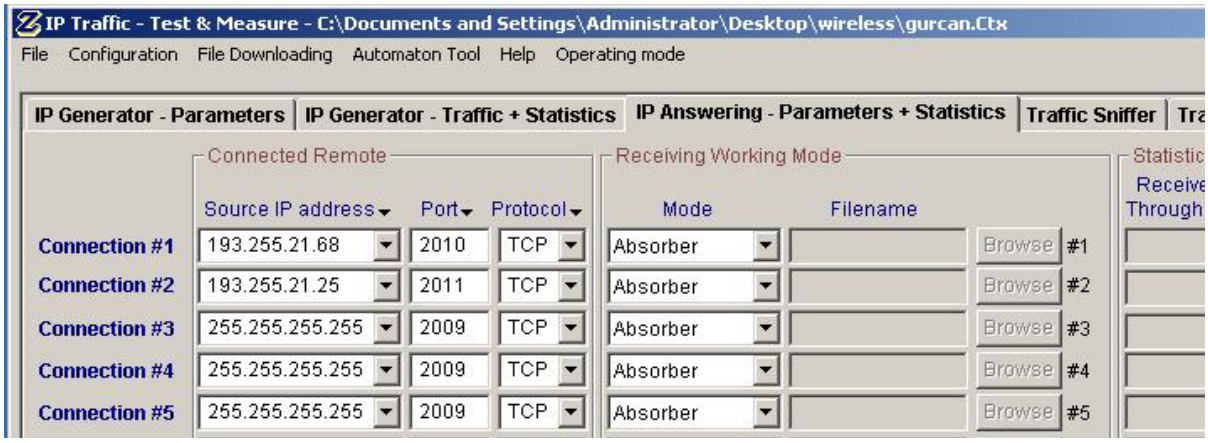
Paketlerin içerikleri rastgele olacak şekilde ayarlanmıştır.

- Paket Uzunluğu

Üretilecek paket uzunlukları gerçek bir ağ gibi davranmasını sağlayabilmek için rastgele olacak şekilde ayarlanmıştır. Daha sonra sırasıyla sabit 100-500-1000-1500 byte uzunluklu paketlerin üretimi ile ayrı ayrı sonuçlar elde edilmiştir.



Şekil 3.14: İstemci tarafında IP Traffic yazılımının Parametrelerinin Ayarlanması



Şekil 3.15: Sunucu tarafında IP Traffic programının Parametrelerinin Ayarlanması

3.6.5. Prosedür

Bu bölümde deneyleri yaparken nasıl bir yol izlendiği, hangi işlemlerin yapıldığı açıklanmaktadır.

Deneyin ilk aşamasında 2 farklı trafik tipi için (TCP ve UDP) yararlı yük (throughput) ve toplam süre (response time) farklı güvenlik mekanizmaları altında ölçülmüştür.

Deneyler öncelikle tek istemcili ardından da iki istemcili bir ağda gerçekleştirilmiştir.

2000 ve 25000 kb/s bant genişliği tıkanıklık oluşmayan ağlar için 55000 kb/s bant genişliği de tıkanıklık oluşabilen ağları gerçekleştirebilmek için kullanılmıştır.

Paket uzunluğu öncelikle rastgele olacak şekilde kullanılmış, daha sonra da 100-500-1000-1500 byte sabit paket uzunlukları kullanılmıştır.

Bu parametrik ayarların her bir unsuru için ve her bir güvenlik mekanizması için yapılan deneyler 5 defa gerçekleştirilmiştir ve sonuçları incelemek için denemelerin ortalamaları alınmıştır.

4. BULGULAR

Bu bölüm, geliştirilen simülasyon programı ile 802.11b/g/i ağların güvenlik mekanizmalarını içeren ve güvenlik mekanizması içermeyen durumlarının performans sonuçlarını içermektedir. İlk olarak 802.11b ağlar için yapılan testlerin konfigürasyonları verilmiş ve elde edilen sonuçlar grafiksel olarak ifade edilmektedir. 802.11i standardı, 802.11g standartının fiziksel özellikleri üzerine geliştirilmiş güvenlik eklentileridir. Bu yüzden 802.11i ve 802.11g için aynı fiziksel ortam konfigürasyonları kullanılmaktadır. Bu konfigürasyonlar kullanılarak yapılan testlerden elde dilen sonuçlar da grafiksel olarak ifade edilmektedir. Bu testlerde Bölüm 3.5.2'de belirtilen 5 farklı güvenlik mekanizmasından uygun olanlar seçilerek gerçekleştirilmiştir.

4.1. 802.11B AĞLAR İÇİN ELDE EDİLEN SONUÇLAR

Yapılan test çalışmalarının ilk kısmı istemci sayısı 2 – 10 aralığında olan küçük boyutlu ağlar için gerçekleştirilmiştir. İkinci kısmı ise istemci sayısı 10-50 aralığında olan orta büyüklükte ağlar için gerçekleştirilmiştir. Bu testler için giriş parametrelerinin değer veya değerleri bir sonraki bölümde belirtilmiştir. Bazı parametrelerin değerleri tüm testler için sabit belirlenirken bazı parametrelerin birden çok değeri kullanılarak testler yapılmıştır.

4.1.1 Giriş Parametreleri

- Simulation Time : 60 br.zaman
- Access Mechanism : Basic Access
- Physical Layer Configuration : 802.11b
- Data Rate Configuration: 5.5 Mbps ve 11 Mbps
- Number of Nodes: 2, 4, 6, 8, 10, 20, 30, 40, 50
- Packet Length Distribution: Constant
- Packet Length Mean : 8000 bit
- Packet Generation Rate Configuration : Constant
- Packet Generation Rate Mean: 8
- Security : No Security, 40 bit Anahtarlı WEP , 104 bit Anahtarlı WEP, WPA

4.1.2. Sonuçlar

802.11b ağlarda 5.5 Mbps ve 11 Mbps hızlar için testler yapılmış ve sonuçlar elde edilmiştir. 11 Mbps hızında yapılan testlerin sonuçları aşağıdaki tablolarda verilmiştir. İncelenen güvenlik düzeyleri Güvenliksiz, 40 bit Anahtarlı WEP, 104 bit Anahtarlı WEP ve WPA'dır. Testler istemci sayısı 2-10 arasında değişen küçük boyutlu ağlar ve istemci sayısı 10-50 arasında değişen büyük boyutlu ağlar için yapılmıştır.

4.1.2.1. Küçük Boyutlu Ağlar

Tablo 4.1 : Küçük Boyutlu 802.11b (11 Mbps) Ağlar için Geçen Toplam Zaman (sn)

İstemci Sayısı	Güvenliksiz	WEP(40)	WEP(104)	WPA
2	37,500	38,109	38,593	40,125
4	82,563	84,219	84,235	89,123
6	140,282	143,750	143,906	147,214
8	216,047	221,344	223,297	224,545
10	313,109	319,656	320,891	322,123

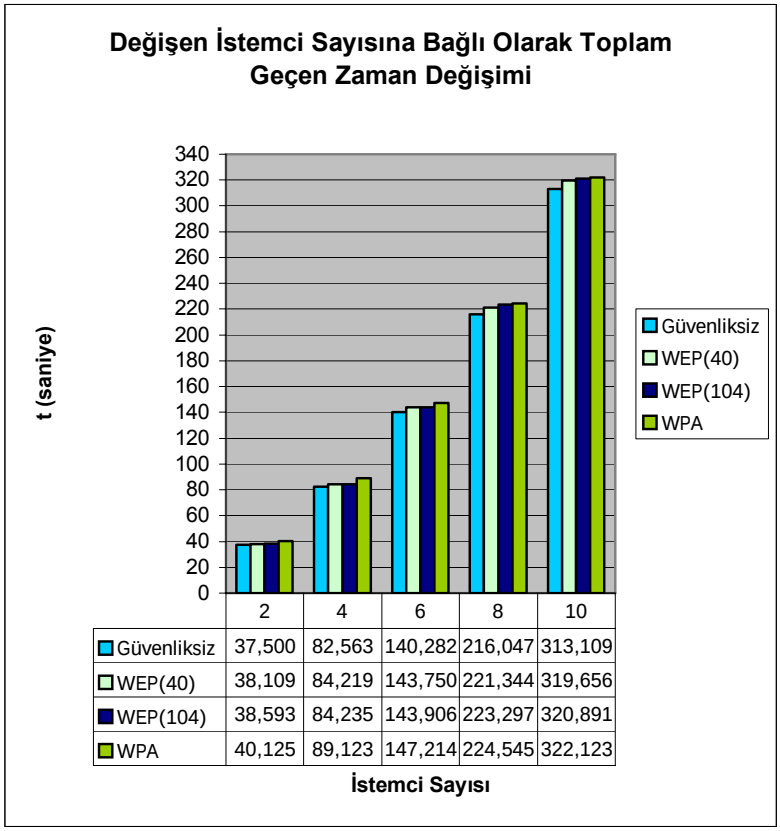
4.1.2.2. Büyük Boyutlu Ağlar

Tablo 4.2 : Büyük Boyutlu 802.11b (11 Mbps) Ağlar için Geçen Toplam Zaman (sn)

İstemci Sayısı	Güvenliksiz	WEP(40)	WEP(104)	WPA
10	313,109	319,656	320,891	322,123
20	1437,703	1454,125	1458,671	1463,120
30	4804,984	4887,579	5310,781	5358,019
40	12312,109	12379,656	12421,241	12432,985
50	26842,516	26884,797	27129,797	27612,000

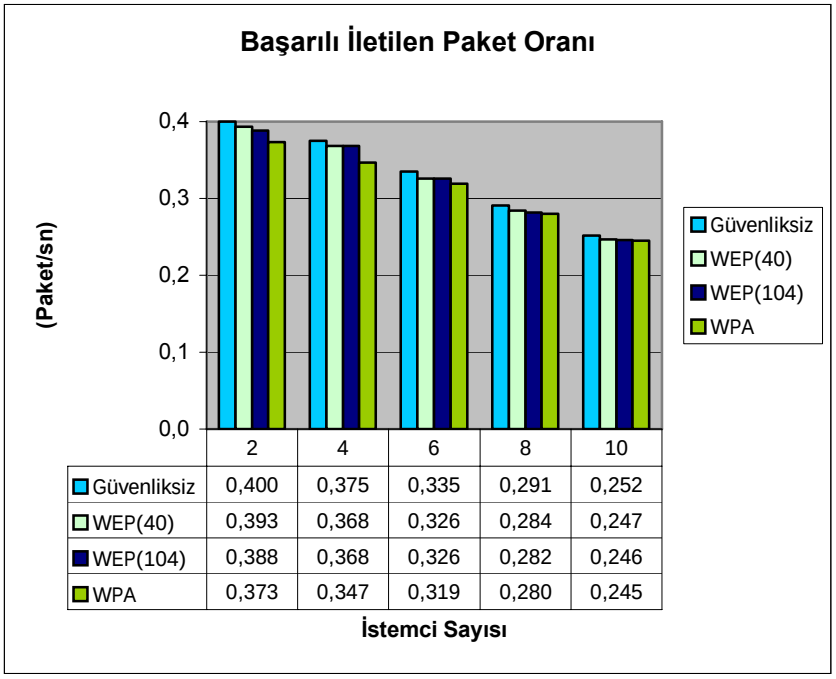
4.1.3. Grafikler

4.1.3.1. Küçük Boyutlu Ağlar



	2	4	6	8	10
Güvenliksiz	37,500	82,563	140,282	216,047	313,109
WEP(40)	38,109	84,219	143,750	221,344	319,656
WEP(104)	38,593	84,235	143,906	223,297	320,891
WPA	40,125	89,123	147,214	224,545	322,123

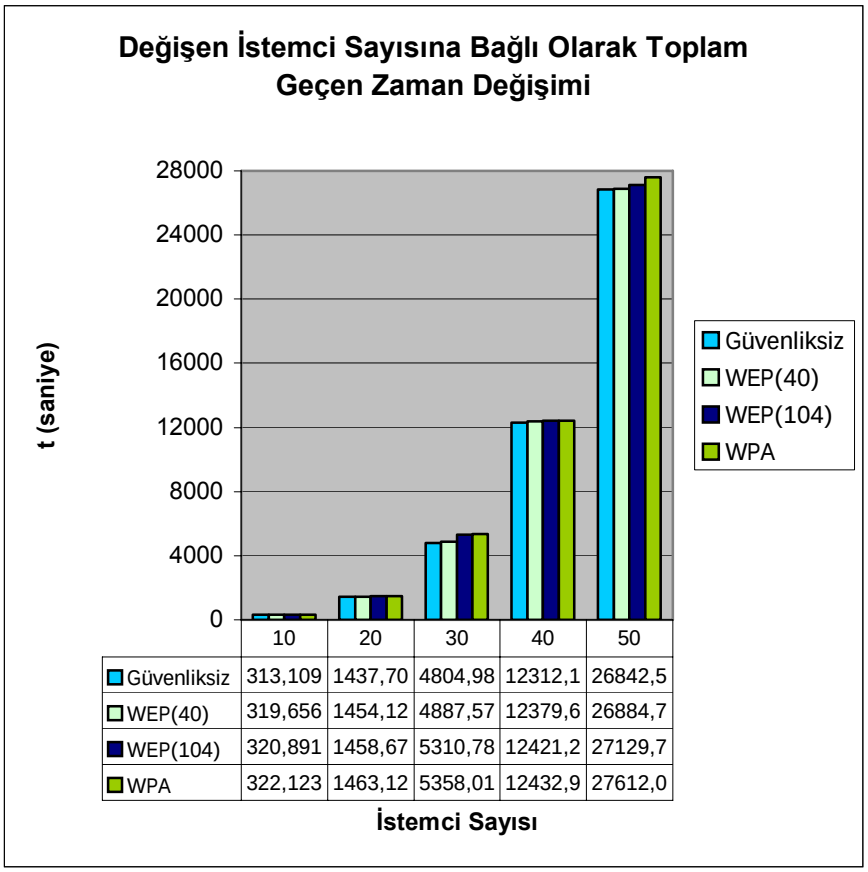
Şekil 4.1 : Küçük boyutlu 802.11b (11 Mbps) için Zaman Cinsinden Performans Değişimi



	2	4	6	8	10
Güvenliksiz	0,400	0,375	0,335	0,291	0,252
WEP(40)	0,393	0,368	0,326	0,284	0,247
WEP(104)	0,388	0,368	0,326	0,282	0,246
WPA	0,373	0,347	0,319	0,280	0,245

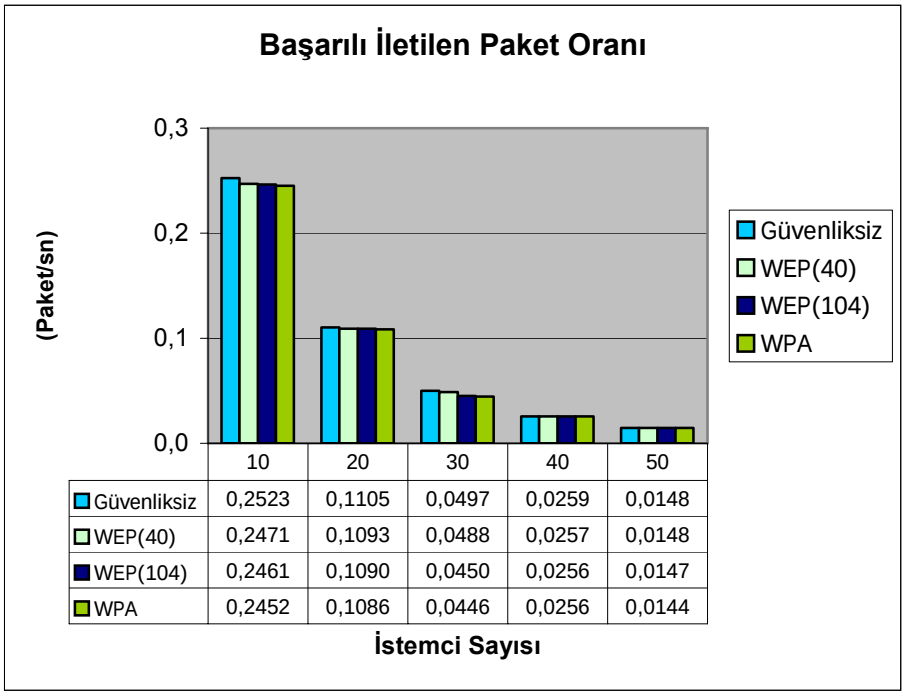
Şekil 4.2 : Küçük boyutlu 802.11b (11 Mbps) için Başarılı İletilen Paket Oranı

4.1.3.2. Büyük Boyutlu Ağlar



	10	20	30	40	50
Güvenliksiz	313,109	1437,70	4804,98	12312,1	26842,5
WEP(40)	319,656	1454,12	4887,57	12379,6	26884,7
WEP(104)	320,891	1458,67	5310,78	12421,2	27129,7
WPA	322,123	1463,12	5358,01	12432,9	27612,0

Şekil 4.3 : Büyük boyutlu 802.11b (11 Mbps) için Zaman Cinsinden Performans Değişimi



	10	20	30	40	50
Güvenliksiz	0,2523	0,1105	0,0497	0,0259	0,0148
WEP(40)	0,2471	0,1093	0,0488	0,0257	0,0148
WEP(104)	0,2461	0,1090	0,0450	0,0256	0,0147
WPA	0,2452	0,1086	0,0446	0,0256	0,0144

Şekil 4.4 : Büyük boyutlu 802.11b (11 Mbps) Ağlar için Başarılı İletilen Paket Oranı

4.1. 802.11G AĞLAR İÇİN ELDE EDİLEN SONUÇLAR

Bu tip ağlar için test çalışmaları ilk önce istemci sayısı 2 – 10 aralığında olan küçük boyutlu ağlar için gerçekleştirilmiştir. İkinci kısmı ise istemci sayısı 10-50 aralığında olan orta büyüklükte ağlar için gerçekleştirilmiştir. Bu testler için giriş parametrelerinin değer veya değerleri bir sonraki bölümde belirtilmiştir. Bazı parametrelerin değerleri tüm testler için sabit belirlenirken bazı parametrelerin birden çok değeri kullanılarak testler yapılmıştır.

4.2.1 Giriş Parametreleri

- Simulation Time : 60 br.zaman
- Access Mechanism : Basic Access
- Physical Layer Configuration : 802.11g ve 802.11i
- Data Rate Configuration: 6 Mbps, 12 Mbps, 36 Mbps, 48 Mbps ve 54 Mbps
- Number of Nodes: 2, 4, 6, 8, 10, 20, 30, 40, 50
- Packet Length Distribution: Constant ve Exponential
- Packet Length Mean : 8000 bit
- Packet Generation Rate Configuration : Constant
- Packet Generation Rate Mean: 8
- Security : No Security, WEP (40), WEP (104), WPA , WPA2

4.2.2. Sonuçlar

802.11b ağlarda 6 Mbps, 12 Mbps, 36 Mbps, 48 Mbps ve 54 Mbps hızlar için testler yapılmış ve sonuçlar elde edilmiştir. İncelenen güvenlik dzeyleri Güvenliksiz, 40 bit Anahtarlı WEP, 104 bit Anahtarlı WEP , WPA ve WPA2'dir. Testler istemci sayısı 2-10 arasında değişen küçük ve 10-50 arasında değişen büyük ağlar için yapılmıştır.

4.2.2.1. Küçük Boyutlu Ağlar

Tablo 4.3 : Küçük Boyutlu 802.11g (12 Mbps) Ağlar için Geçen Toplam Zaman (sn)

İstemci Sayısı	Güvenliksiz	WEP(40)	WEP(104)	WPA	WPA2
2	17,297	17,302	17,415	17,578	18,406
4	38,281	38,400	38,685	38,906	40,547
6	63,671	63,989	64,125	64,547	67,250
8	95,328	95,985	96,125	96,703	99,890
10	134,953	135,010	135,120	135,140	140,516

Tablo 4.4 : Küçük Boyutlu 802.11g (36 Mbps) Ağlar için Geçen Toplam Zaman (sn)

İstemci Sayısı	Güvenliksiz	WEP(40)	WEP(104)	WPA	WPA2
2	17,250	17,252	17,285	17,297	18,141
4	36,937	36,989	37,252	37,641	39,047
6	59,953	59,899	60,212	60,531	63,657
8	86,563	86,865	87,012	87,172	91,047
10	118,125	118,325	118,765	118,906	124,125

Tablo 4.5 : Küçük Boyutlu 802.11g (54 Mbps) Ağlar için Geçen Toplam Zamanı (sn)

İstemci Sayısı	Güvenliksiz	WEP(40)	WEP(1049	WPA	WPA2
2	17,031	17,102	17,165	17,187	18,871
4	36,171	36,256	36,452	36,563	38,343
6	58,563	58,625	58,712	58,797	61,531
8	83,718	83,989	84,212	84,578	88,265
10	113,766	114,000	114,652	114,750	119,218

4.2.2.2. Büyük Boyutlu Ağlar

Tablo 4.6 : Büyük Boyutlu 802.11g (12 Mbps) Ağlar için Geçen Toplam Zaman (sn)

İstemci Sayısı	Güvenliksiz	WEP(40)	WEP(104)	WPA	WPA2
10	134,953	135,010	135,120	135,140	140,516
20	531,922	532,123	533,010	533,156	541,172
30	2366,078	2376,066	2392,452	2407,734	2411,000
40	4266,250	4270,796	4284,695	4287,641	4292,047
50	9444,484	9451,841	9472,512	9495,672	9772,046

Tablo 4.7 : Büyük Boyutlu 802.11g (36 Mbps) Ağlar için Geçen Toplam Zaman (sn)

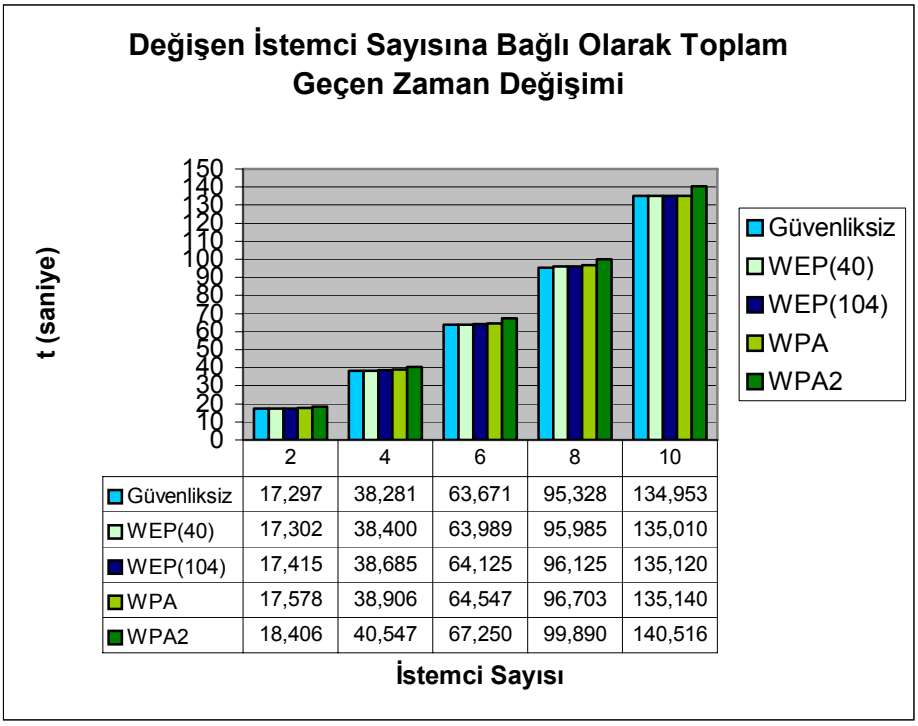
İstemci Sayısı	Güvenliksiz	WEP(40)	WEP(104)	WPA	WPA2
10	118,125	118,325	118,765	118,906	124,125
20	371,078	372,198	372,985	374,937	383,422
30	960,500	962,532	963,996	964,234	979,672
40	2173,766	2173,989	2175,012	2175,813	2214,297
50	4458,109	4462,845	4466,013	4467,406	4545,547

Tablo 4.8 : Büyük Boyutlu 802.11g (54 Mbps) Ağlar için Geçen Toplam Zaman (sn),

İstemci Sayısı	Güvenliksiz	WEP(40)	WEP(104)	WPA	WPA2
10	113,766	114,000	114,652	114,750	119,218
20	343,453	344,120	345,010	345,375	354,297
30	846,828	847,030	848,014	848,641	864,032
40	1822,046	1825,042	1828,014	1831,813	1841,140
50	3592,953	3598,985	3604,150	3611,188	3626,125

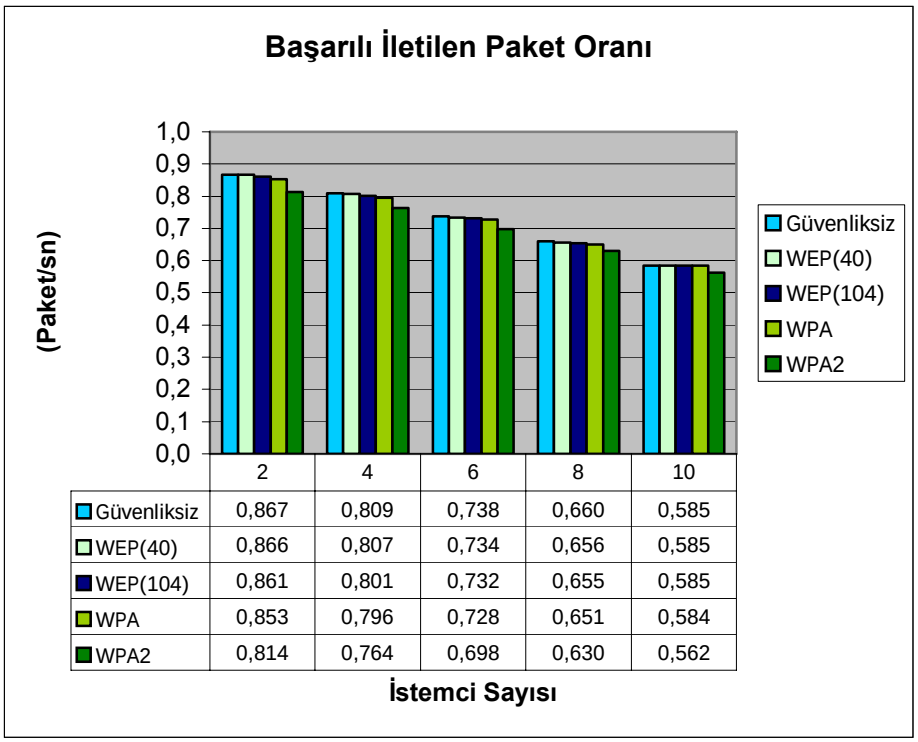
4.2.3. Grafikler

4.2.2.1. Küçük Boyutlu Ağlar



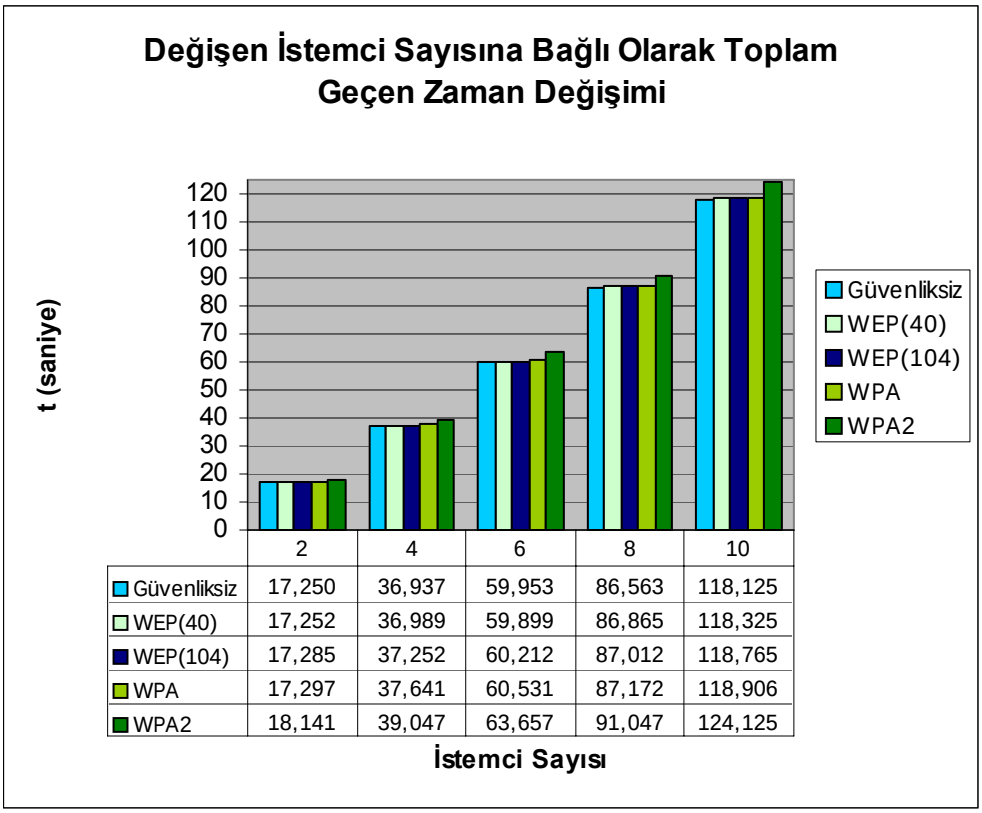
	2	4	6	8	10
Güvenliksiz	17,297	38,281	63,671	95,328	134,953
WEP(40)	17,302	38,400	63,989	95,985	135,010
WEP(104)	17,415	38,685	64,125	96,125	135,120
WPA	17,578	38,906	64,547	96,703	135,140
WPA2	18,406	40,547	67,250	99,890	140,516

Şekil 4.5 : Küçük Boyutlu 802.11g (12 Mbps) için Zaman Cinsinden Performans Değişimi



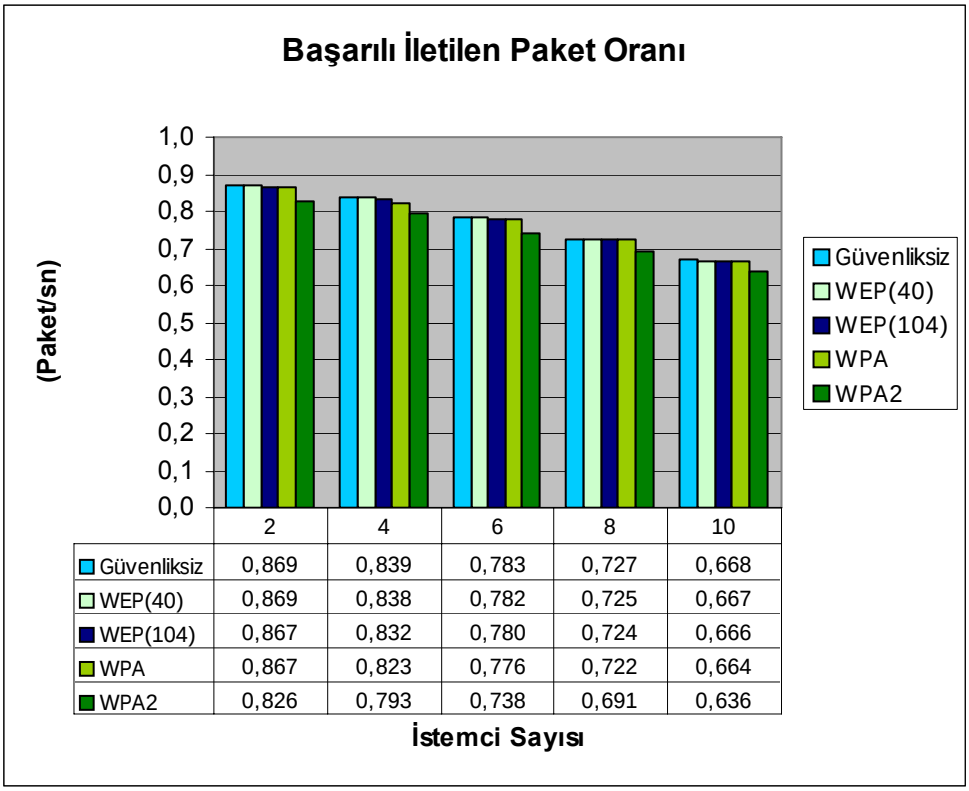
	2	4	6	8	10
Güvenliksiz	0,867	0,809	0,738	0,660	0,585
WEP(40)	0,866	0,807	0,734	0,656	0,585
WEP(104)	0,861	0,801	0,732	0,655	0,585
WPA	0,853	0,796	0,728	0,651	0,584
WPA2	0,814	0,764	0,698	0,630	0,562

Şekil 4.6 : Küçük Boyutlu 802.11g (12 Mbps) için sistemdeki Başarılı İletilen Paket Oranı



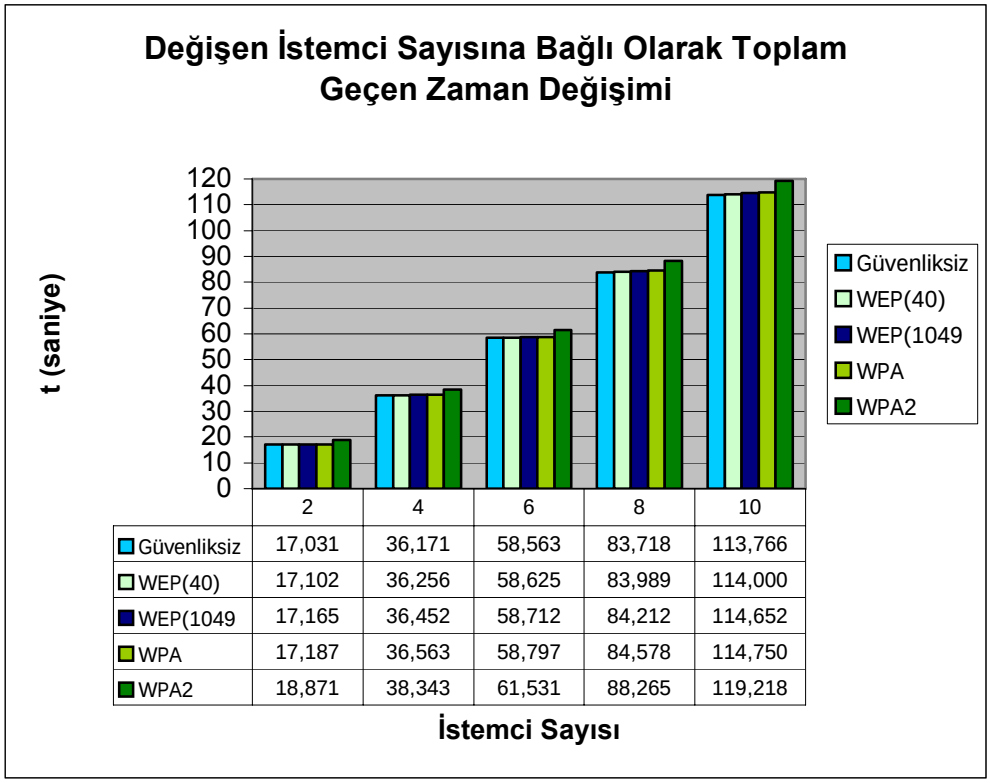
	2	4	6	8	10
Güvenliksiz	17,250	36,937	59,953	86,563	118,125
WEP(40)	17,252	36,989	59,899	86,865	118,325
WEP(104)	17,285	37,252	60,212	87,012	118,765
WPA	17,297	37,641	60,531	87,172	118,906
WPA2	18,141	39,047	63,657	91,047	124,125

Şekil 4.7 : Küçük Boyutlu 802.11g (36 Mbps) için Zaman Cinsinden Performans Değişimi



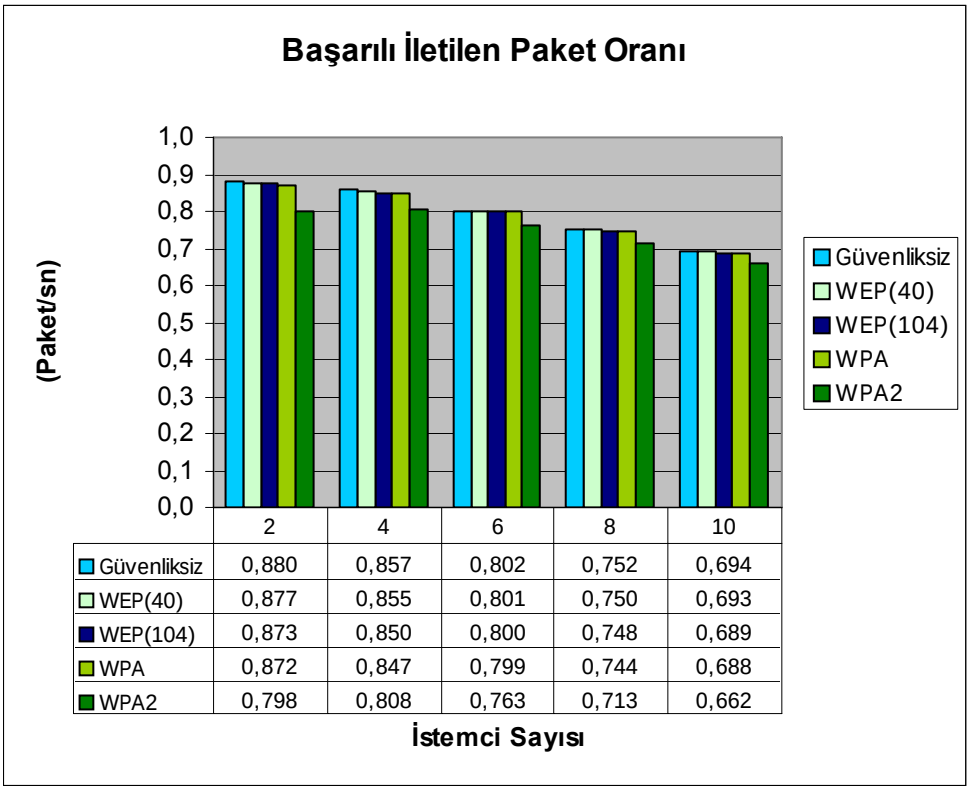
	2	4	6	8	10
Güvenliksiz	0,869	0,839	0,783	0,727	0,668
WEP(40)	0,869	0,838	0,782	0,725	0,667
WEP(104)	0,867	0,832	0,780	0,724	0,666
WPA	0,867	0,823	0,776	0,722	0,664
WPA2	0,826	0,793	0,738	0,691	0,636

Şekil 4.8 : Küçük Boyutlu 802.11g (36 Mbps) için sistemdeki Başarılı İletilen Paket Oranı



	2	4	6	8	10
Güvenliksiz	17,031	36,171	58,563	83,718	113,766
WEP(40)	17,102	36,256	58,625	83,989	114,000
WEP(1049	17,165	36,452	58,712	84,212	114,652
WPA	17,187	36,563	58,797	84,578	114,750
WPA2	18,871	38,343	61,531	88,265	119,218

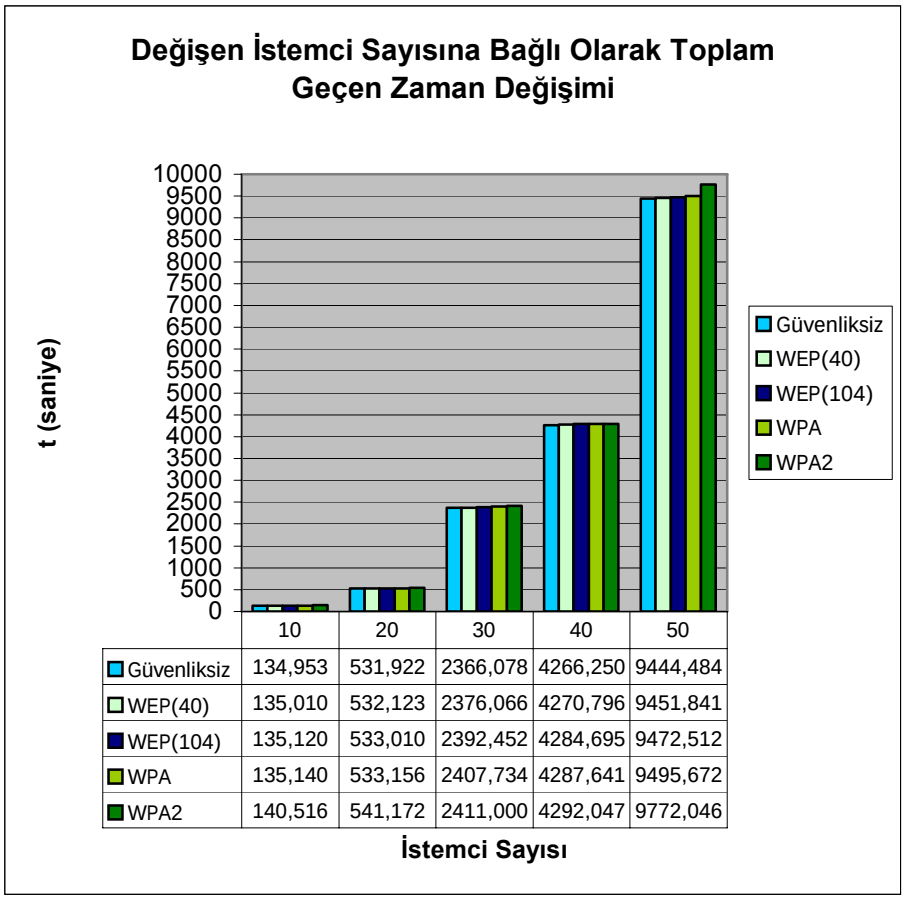
Şekil 4.9 : Küçük Boyutlu 802.11g (54 Mbps) için Zaman Cinsinden Performans Değişimi



	2	4	6	8	10
Güvenliksiz	0,880	0,857	0,802	0,752	0,694
WEP(40)	0,877	0,855	0,801	0,750	0,693
WEP(104)	0,873	0,850	0,800	0,748	0,689
WPA	0,872	0,847	0,799	0,744	0,688
WPA2	0,798	0,808	0,763	0,713	0,662

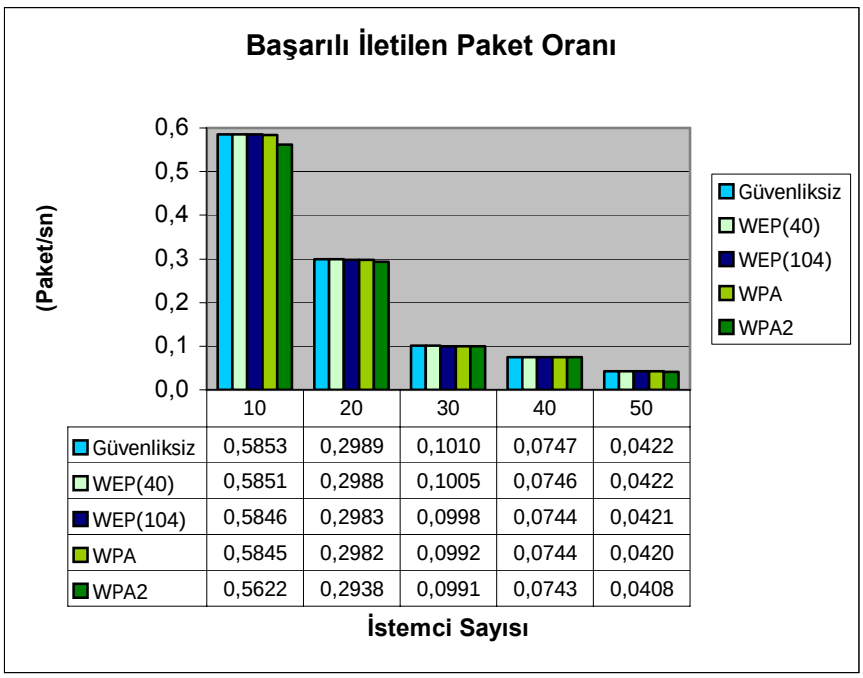
Şekil 4.10 : Küçük Boyutlu 802.11g (54 Mbps) için sistemdeki Başarılı İletilen Paket Oranı

4.2.2.2. Büyük Boyutlu Ağlar



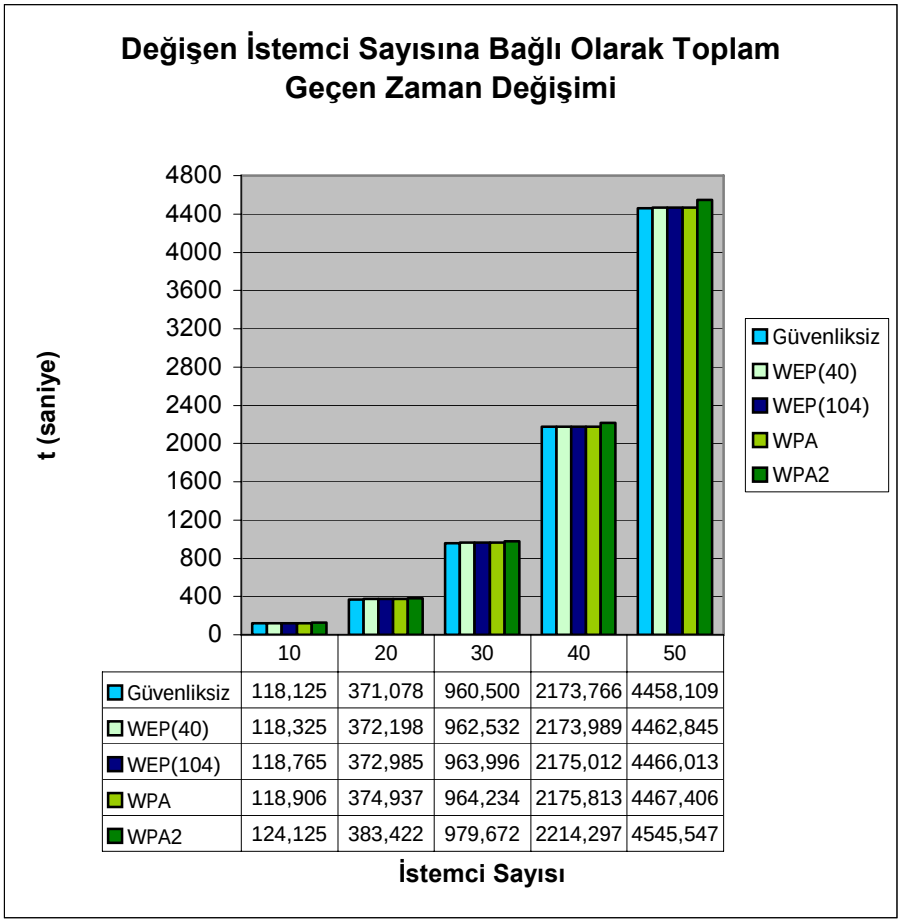
	10	20	30	40	50
Güvenliksiz	134,953	531,922	2366,078	4266,250	9444,484
WEP(40)	135,010	532,123	2376,066	4270,796	9451,841
WEP(104)	135,120	533,010	2392,452	4284,695	9472,512
WPA	135,140	533,156	2407,734	4287,641	9495,672
WPA2	140,516	541,172	2411,000	4292,047	9772,046

Şekil 4.11 : Büyük Boyutlu 802.11g (12 Mbps) için Zaman Cinsinden Performans Değişimi



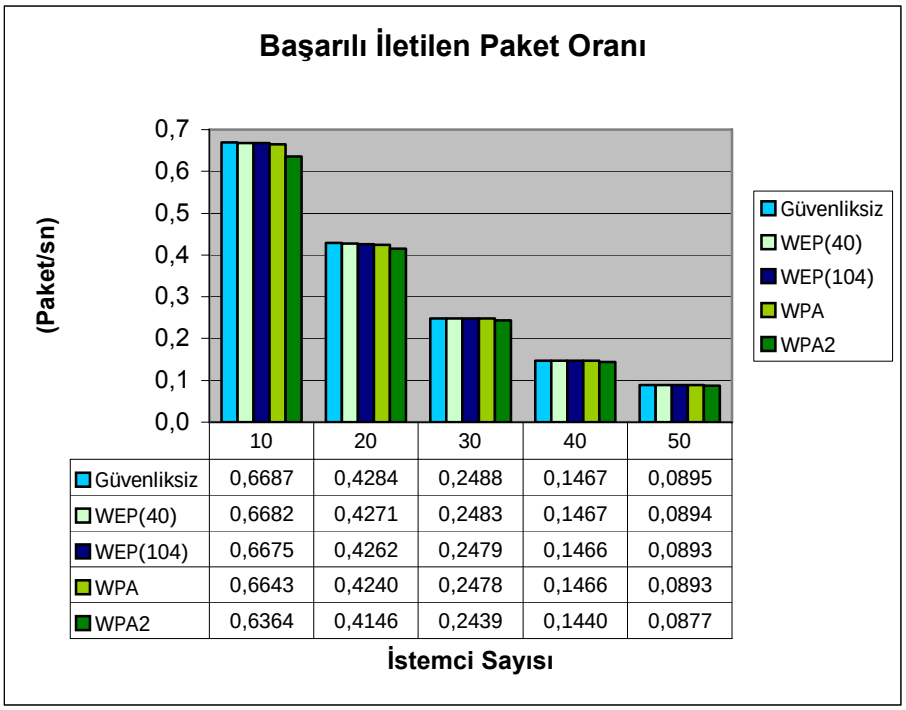
	10	20	30	40	50
Güvenliksiz	0,5853	0,2989	0,1010	0,0747	0,0422
WEP(40)	0,5851	0,2988	0,1005	0,0746	0,0422
WEP(104)	0,5846	0,2983	0,0998	0,0744	0,0421
WPA	0,5845	0,2982	0,0992	0,0744	0,0420
WPA2	0,5622	0,2938	0,0991	0,0743	0,0408

Şekil 4.12 : Büyük Boyutlu 802.11g (12 Mbps) için sistemdeki Başarılı İletilen Paket Oranı



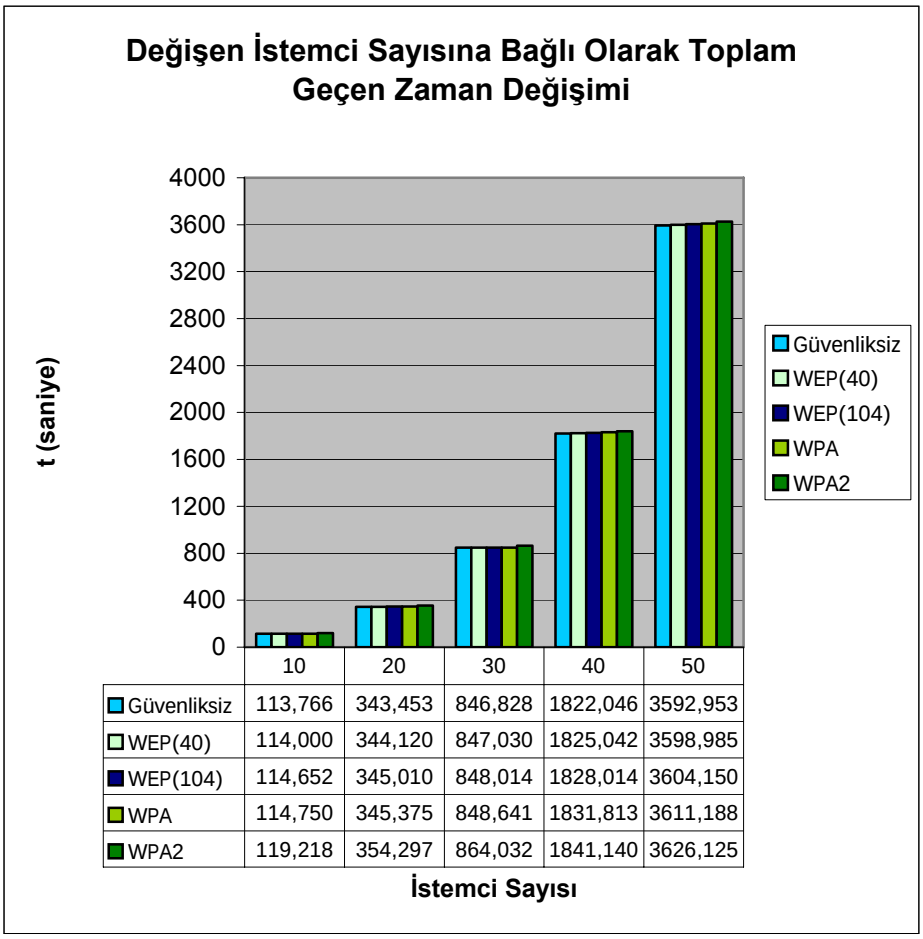
	10	20	30	40	50
Güvenliksiz	118,125	371,078	960,500	2173,766	4458,109
WEP(40)	118,325	372,198	962,532	2173,989	4462,845
WEP(104)	118,765	372,985	963,996	2175,012	4466,013
WPA	118,906	374,937	964,234	2175,813	4467,406
WPA2	124,125	383,422	979,672	2214,297	4545,547

Şekil 4.13 : Büyük Boyutlu 802.11g (36 Mbps) için Zaman Cinsinden Performans Değişimi



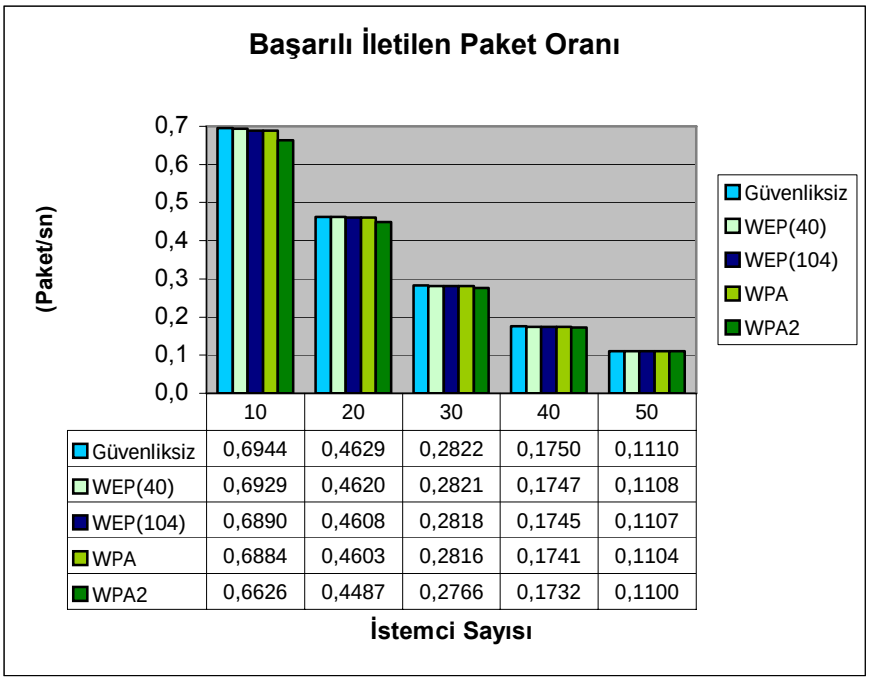
	10	20	30	40	50
Güvenliksiz	0,6687	0,4284	0,2488	0,1467	0,0895
WEP(40)	0,6682	0,4271	0,2483	0,1467	0,0894
WEP(104)	0,6675	0,4262	0,2479	0,1466	0,0893
WPA	0,6643	0,4240	0,2478	0,1466	0,0893
WPA2	0,6364	0,4146	0,2439	0,1440	0,0877

Şekil 4.14 : Büyük Boyutlu 802.11g (36 Mbps) için sistemdeki Başarılı İletilen Paket Oranı



	10	20	30	40	50
Güvenliksiz	113,766	343,453	846,828	1822,046	3592,953
WEP(40)	114,000	344,120	847,030	1825,042	3598,985
WEP(104)	114,652	345,010	848,014	1828,014	3604,150
WPA	114,750	345,375	848,641	1831,813	3611,188
WPA2	119,218	354,297	864,032	1841,140	3626,125

Şekil 4.15 : Büyük Boyutlu 802.11g (54 Mbps) için Zaman Cinsinden Performans Değişimi

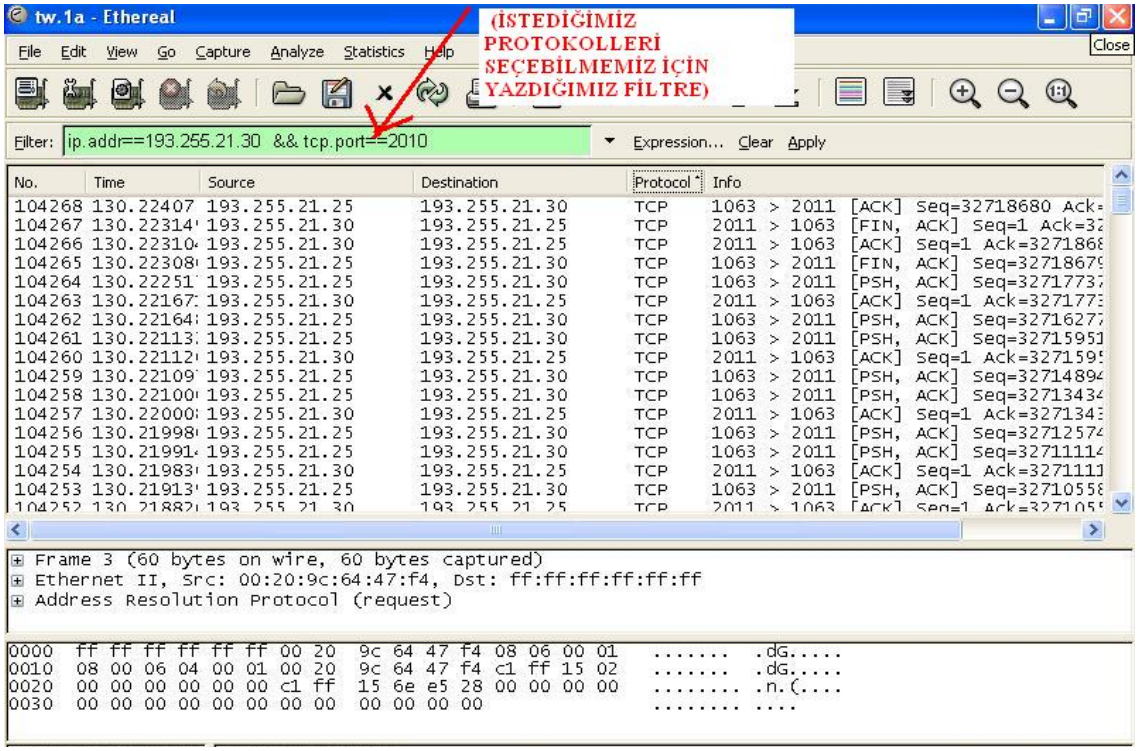


	10	20	30	40	50
Güvenliksiz	0,6944	0,4629	0,2822	0,1750	0,1110
WEP(40)	0,6929	0,4620	0,2821	0,1747	0,1108
WEP(104)	0,6890	0,4608	0,2818	0,1745	0,1107
WPA	0,6884	0,4603	0,2816	0,1741	0,1104
WPA2	0,6626	0,4487	0,2766	0,1732	0,1100

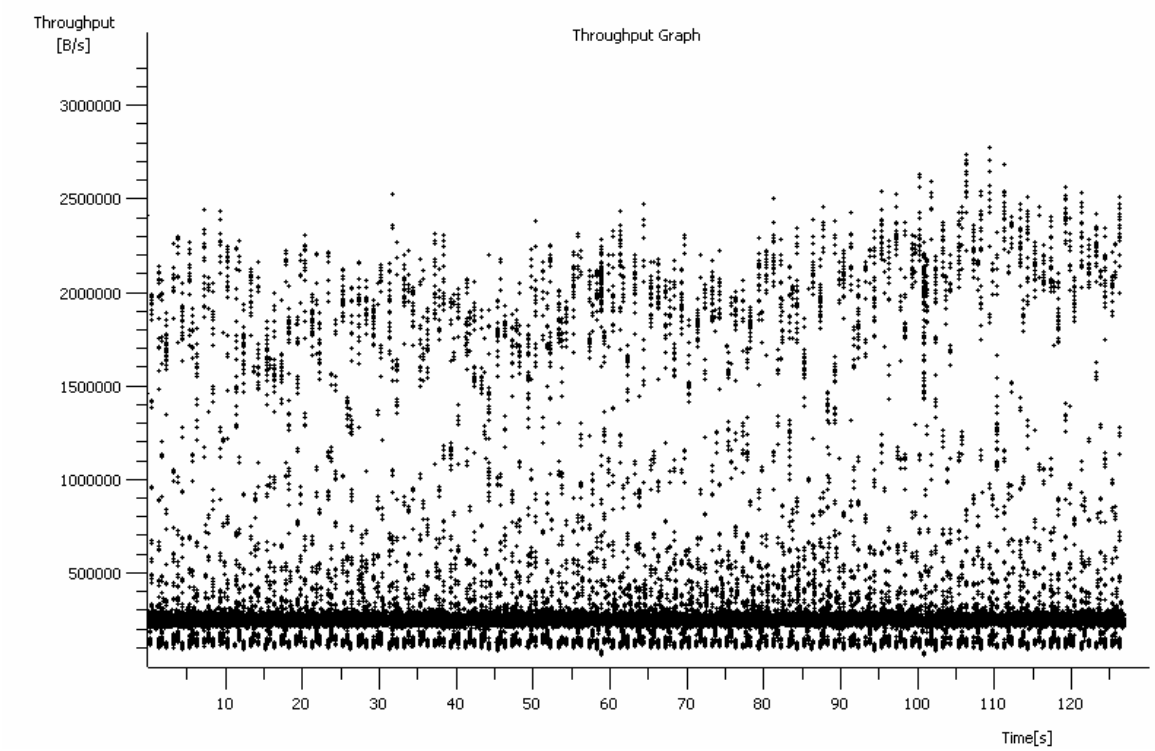
Şekil 4.16 : Büyük Boyutlu 802.11g (54 Mbps) için sistemdeki Başarılı İletilen Paket Oranı

4.3. DENEYSEL ÇALIŞMADAN ELDE EDİLEN SONUÇLAR

Deneylerde bölüm 3.6'da belirtildiği üzere 6 güvenlik katmanı kullanılmıştır. Altyapı WLAN modeline uygun olarak bir adet erişim noktası ve 1 veya 2 istemciden oluşan ağ modeli kullanılmıştır. Her güvenlik mekanizması için farklı trafik tipleri (TCP-UDP) ve farklı sayıda istemciler için denemeler yapılmıştır. IP Traffic yazılımı ile oluşturulan trafik gerçel zamanlı olarak Ethereal yazılımı (Şekil 4.15) ile log dosyaları alınarak incelenmiştir.



Şekil 4.15 : Ethereal yazılımı ile alınmış bir log dosyası



Şekil 4.16 : Ethereal programı ile alınmış bir log dosyası-throughput grafiği

4.3.1. Farklı güvenlik mekanizmalarının performansa etkisi

İlk bölümde tıkanıklık oluşmayan ve bant genişliğini 2000 Kb/s olarak ayarlanan deneylerde elde edilen sonuçlar bu bölümde verilmiştir. Farklı bant genişliklei ile yapılan deney sonuçlarınun tamamaı EK-B'da bulunmaktadır.

Bütün güvenlik katmanları için ve TCP ve UDP protokollerinin kullanıldığı deney sonuçlarının değerleri ayrı ayrı gösterilmektedir.

Tablo 4.9 : Güvenliksiz sistemde TCP -UDP için Throughput-Response Time Değerleri

Security Layer	***Outgoing Bandwidth***	***Packet Length***	***# of client***	***TCP Throughput (Kbytes/sec)***	***TCP Response Time(sec)***
1	2000	Random	1	69,819	139,981
1	2000	Fix 100	1	72,036	68,983
1	2000	Fix 500	1	72,088	110,77
1	2000	Fix 1000	1	76,71	168,042
1	2000	Fix 1500	1	72,857	254,684
Security Layer	***Outgoing Bandwidth***	***Packet Length***	***# of client***	***UDP Throughput (Kbytes/sec)***	***UDP Response Time(sec)***
1	2000	Random	1	82,871	130,01
1	2000	Fix 100	1	87,677	25,527
1	2000	Fix 500	1	87,367	87,2
1	2000	Fix 1000	1	89,132	170,979
1	2000	Fix 1500	1	88,83	285,51

Tablo 4.10 : WEP 64 bit , TCP - UDP için Throughput-Response Time değerleri

Security Layer	***Outgoing Bandwidth***	***Packet Length***	***# of client***	***TCP Throughput (Kbytes/sec)***	***TCP Response Time(sec)***
2	2000	Random	1	64,443	721,981
2	2000	Fix 100	1	66,489	408,923
2	2000	Fix 500	1	66,537	520,751
2	2000	Fix 1000	1	70,803	974,042
2	2000	Fix 1500	1	67,247	1004,672
Security Layer	***Outgoing Bandwidth***	***Packet Length***	***# of client***	***UDP Throughput (Kbytes/sec)***	***UDP Response Time(sec)***
2	2000	Random	1	76,556	195,15
2	2000	Fix 100	1	80,996	38,295
2	2000	Fix 500	1	80,710	127,54
2	2000	Fix 1000	1	82,340	256,467
2	2000	Fix 1500	1	82,061	428,21

Tablo 4.11 : WEP 128 bit , TCP - UDP için Throughput-Response Time değerleri

Security Layer	***Outgoing Bandwidth***	***Packet Length***	***# of client***	***TCP Throughput (Kbytes/sec)***	***TCP Response Time(sec)***
3	2000	Random	1	62,286	779,76
3	2000	Fix 100	1	64,263	441,72
3	2000	Fix 500	1	64,310	562,68
3	2000	Fix 1000	1	68,433	1053,25
3	2000	Fix 1500	1	64,996	1085,45
Security Layer	***Outgoing Bandwidth***	***Packet Length***	***# of client***	***UDP Throughput (Kbytes/sec)***	***UDP Response Time(sec)***
3	2000	Random	1	79,069	194,152
3	2000	Fix 100	1	83,655	36,215
3	2000	Fix 500	1	83,359	123,154
3	2000	Fix 1000	1	85,043	246,447
3	2000	Fix 1500	1	84,755	438,139

Tablo 4.12 : EAP-TLS, TCP - UDP için Throughput-Response Time değerleri

Security Layer	***Outgoing Bandwidth***	***Packet Length***	***# of client***	***TCP Throughput (Kbytes/sec)***	***TCP Response Time(sec)***
4	2000	Random	1	45,088	139,981
4	2000	Fix 100	1	46,520	68,983
4	2000	Fix 500	1	46,554	110,77
4	2000	Fix 1000	1	49,539	168,042
4	2000	Fix 1500	1	47,050	254,684
Security Layer	***Outgoing Bandwidth***	***Packet Length***	***# of client***	***UDP Throughput (Kbytes/sec)***	***UDP Response Time(sec)***
4	2000	Random	1	56,012	130,01
4	2000	Fix 100	1	59,260	25,527
4	2000	Fix 500	1	59,050	87,2
4	2000	Fix 1000	1	60,243	170,979
4	2000	Fix 1500	1	60,039	285,51

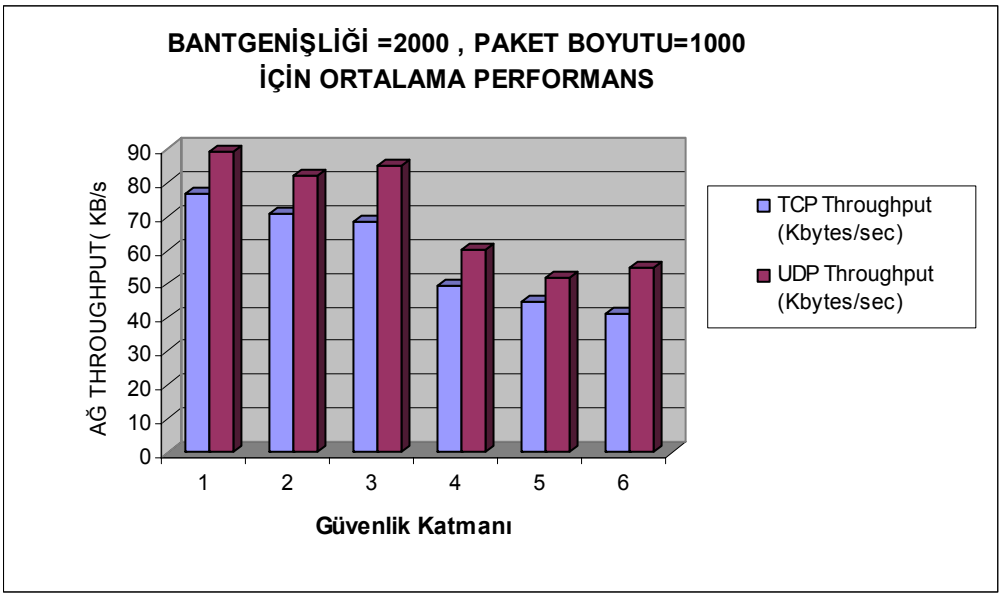
Tablo 4.13 : EAP-TLS-WEP 64 bit, TCP - UDP için Throughput-Response Time değerleri

Security Layer	***Outgoing Bandwidth***	***Packet Length***	***# of client***	***TCP Throughput (Kbytes/sec)***	***TCP Response Time(sec)***
5	2000	Random	1	40,773	746,528
5	2000	Fix 100	1	42,068	422,826
5	2000	Fix 500	1	42,098	538,457
5	2000	Fix 1000	1	44,797	1007,159
5	2000	Fix 1500	1	42,547	1038,831
Security Layer	***Outgoing Bandwidth***	***Packet Length***	***# of client***	***UDP Throughput (Kbytes/sec)***	***UDP Response Time(sec)***
5	2000	Random	1	48,446	198,350
5	2000	Fix 100	1	51,255	38,923
5	2000	Fix 500	1	51,074	129,632
5	2000	Fix 1000	1	52,106	260,673
5	2000	Fix 1500	1	51,929	435,233

Tablo 4.14 : EAP-TLS-WEP 128 bit, TCP - UDP için Throughput-Response Time değerleri

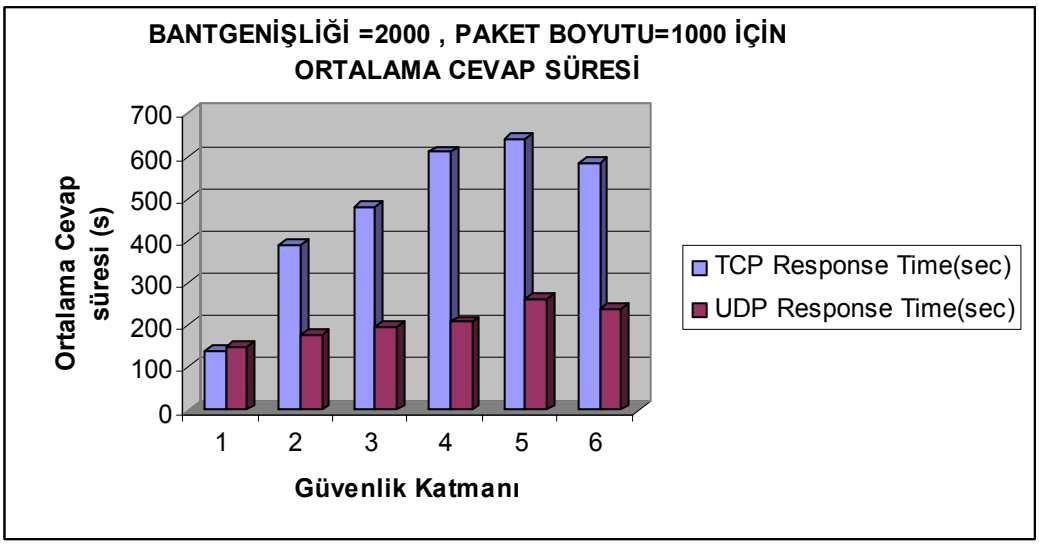
Security Layer	***Outgoing Bandwidth***	***Packet Length***	***# of client***	***TCP Throughput (Kbytes/sec)***	***TCP Response Time(sec)***
6	2000	Random	1	37,562	796,135
6	2000	Fix 100	1	38,755	450,996
6	2000	Fix 500	1	38,783	574,496
6	2000	Fix 1000	1	41,270	1075,368
6	2000	Fix 1500	1	39,197	1108,244
Security Layer	***Outgoing Bandwidth***	***Packet Length***	***# of client***	***UDP Throughput (Kbytes/sec)***	***UDP Response Time(sec)***
6	2000	Random	1	50,999	196,482
6	2000	Fix 100	1	53,956	36,650
6	2000	Fix 500	1	53,766	124,632
6	2000	Fix 1000	1	54,852	249,404
6	2000	Fix 1500	1	54,666	443,397

Elde edilen bu değerler incelendiğinde , tıkanıklık oluşmayan ağlarda güvenlik mekanizmasının seviyesi arttıkça yararlı yük throughput değerinin düştüğü belirlenmiştir. Bu hem TCP hem de UDP protokolü için geçerlidir. Bazı ara değerlerde çok ufak artışlar ve azalmalar gözükmesine rağmen genel gidişatın yukarıdaki gibi olduğunu varsaydığımız zaman bunları istisna olarak kabul edilmiştir.



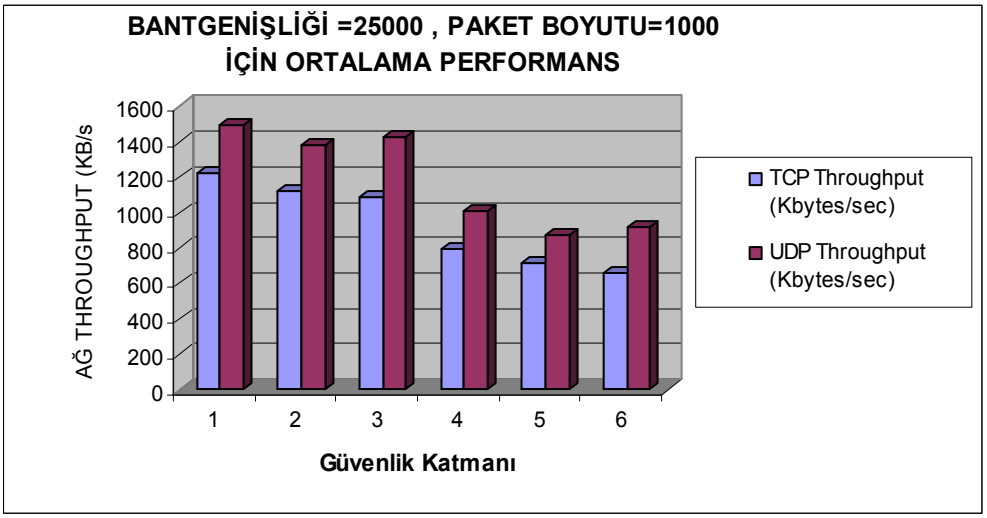
Şekil 4.17 : Tıkanıklık olmayan ağda BW=2000 kb/s, farklı güvenlik mekanizmaları için TCP-UDP Throughput değerleri

Toplam geçen zamanı incelediğimizde ise yararlı yük değişimine benzeyen bir durum söz konusu değildir. İstisnalar olmasına rağmen genel olarak incelendiğinde güvenlik mekanizmasında WEP algoritmasının aktif olduğu yerlerde cevap süresinin daha fazla olduğu görülmektedir.

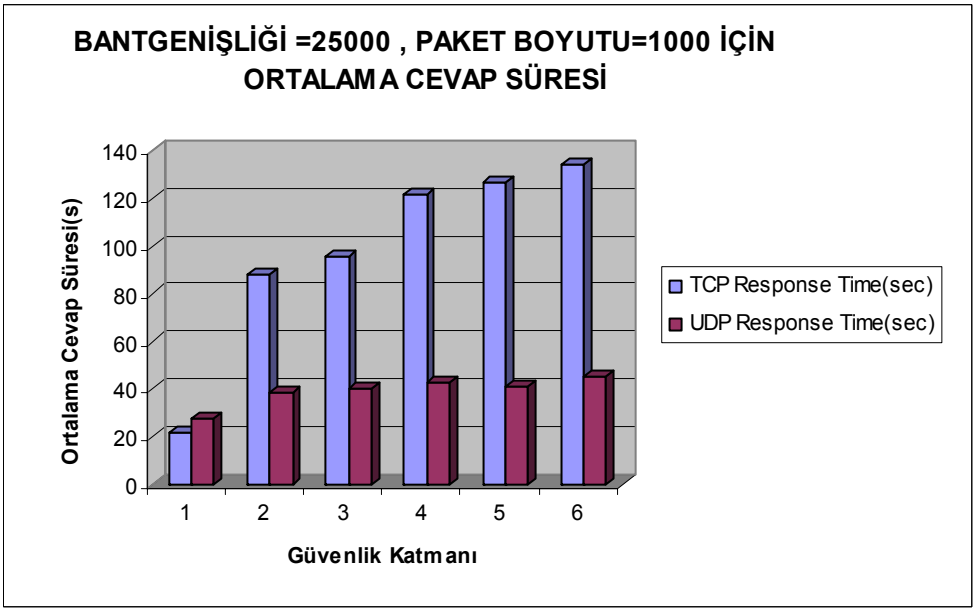


Şekil 4.18 : Tıkanıklık olmayan ağda BW=2000 kb/s, farklı güvenlik mekanizmaları için TCP-UDP ortalama cevap süreleri

Deneyin ikinci aşamasında , bant genişliğini 25000 Kb/s olarak ayarlanmıştır. Bu durumda yine tıkanıklık oluşmayan bir ağ tipi incelenmesine rağmen 2000 kb/s bant genişliğinde elde ettiğimiz sonuçlardan farklı sonuçlar elde edilmiştir. Fakat bu verileri karşılaştırdığımıda genel itibariyle benzer sonuçlar verdiği görülmüştür. Bu deneylerde bulunan tüm sonuçlar EK-B'de verilmiştir.

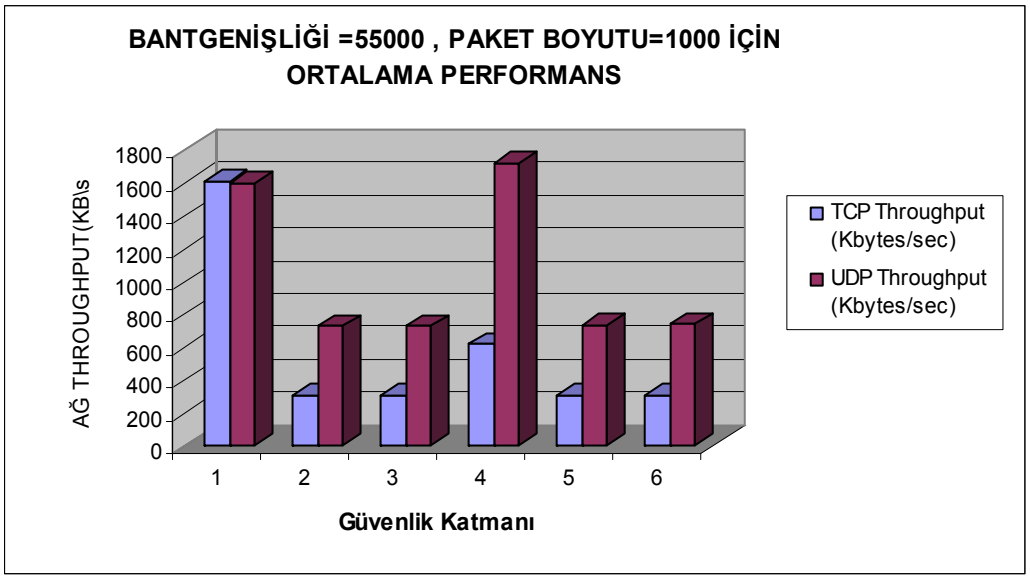


Şekil 4.19 : Tıkanıklık olmayan ağda BW=25000 kb/s farklı güvenlik mekanizmaları için TCP-UDP Throughput değerleri

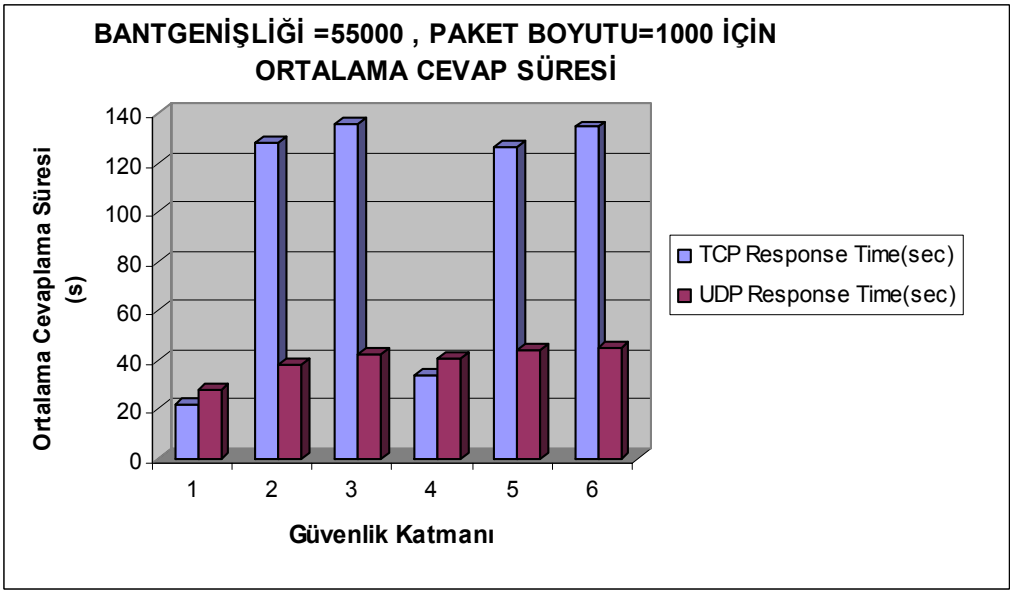


Şekil 4.20 : Tıkanıklık olmayan ağda BW=25000 kb/s farklı güvenlik mekanizmaları için TCP-UDP ortalama cevap süreleri

Deneyin üçüncü aşamasında , tıkanıklı oluşabilen bir ağ tipini inceleyebilmek için bant genişliğini 55500 Kb/s olarak ayarlanmıştır. Deneyde bulunan değerleri aşağıdaki tablo TCP ve UDP için ayrı ayrı göstermektedir Bu deneylerde bulunan tüm sonuçlar EK-B'de verilmiştir.



Şekil 4.21 : Tıkanıklık olmayan ağda BW=55000 kb/s, farklı güvenlik mekanizmaları için TCP-UDP Throughput değerleri



Şekil 4.22 : Tıkanıklık olmayan ağda BW=55000 kb/s, farklı güvenlik mekanizmaları için TCP-UDP ortalama cevap süreleri

Bu bölümde farklı güvenlik katmanları ve farklı bant genişlikleri kullanılarak gerçekleştirilen deneylerin sonuçlarına yer verilmiştir. Bu deneylerde paket boyutu 1000 olarak belirlenmiştir. Paket boyutlarının sistem performansına etkisi bölüm 4.3.3 'de açıklanmıştır. Deney bilgileri incelendiğinde aşağıdaki sonuçlar çıkarılabilir.

Tıkanıklık oluşmayan ağlarda güvenlik mekanizmasının seviyesi arttıkça yararlı yük throughput değerinin düştüğü belirlenmiştir. Benzer bir sonuç beklenirken WEP algoritmasını şifreleme amacıyla kullanan 2-3-5-6 numaralı güvenlik katmanlarının uygulandığı sistemlerde throughput'un diğerlerinden daha düşük olduğunu görülmüştür. Bu hem TCP hem de UDP için geçerlidir. Daha önce de belirtildiği gibi arada bazı ara değerlerde çok ufak artışlar ve azalmalar gözükmesine rağmen genel gidişatın yukarıdaki gibi olduğunu varsaydığımız zaman bunları istisna olarak kabul edilmiştir.

Ortalama cevap süresi incelendiği zamanda throughput'a benzeyen bir durum söz konusudur. Genel itibariyle istisnalar sayılmaz ise güvenlik mekanizmasında WEP algoritmasının aktif olduğu yerlerde ortalama cevap süresinin daha fazla olduğu görülmektedir.

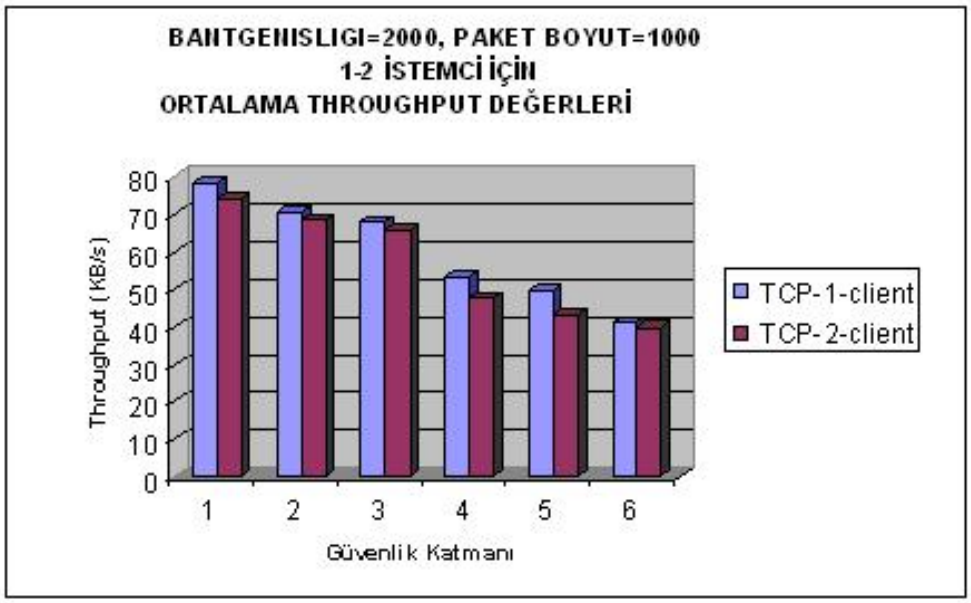
TCP ve UDP protokollerinin performansı karşılaştırılırsa tıkanık olmayan sistemlerde UDP'nin throughput değeri TCP'ye göre biraz daha fazla olduğu gözlenmiştir. Bu miktar TCP throughput değeri, UDP throughput değerinin % 94.68'i kadardır. Tıkanıklık oluşan sistemlerde TCP protokolü bağlantıya dayalı bir protokol olduğu için ve tıkanıklık kontrolü gerçekleştirdiği için UDP protokolünden daha yavaştır. Özellikle WEP algoritmasının uygulandığı yerlerde daha da yavaş olduğu gözükmektedir. TCP throughput WEP uygulanan yerlerde UDP throughput'un %19,82'si kadarken, WEP uygulanmayan yerlerde %88.23'si kadardır.

4.3.2. Birden fazla istemci eklenmesinin performansa etkisi

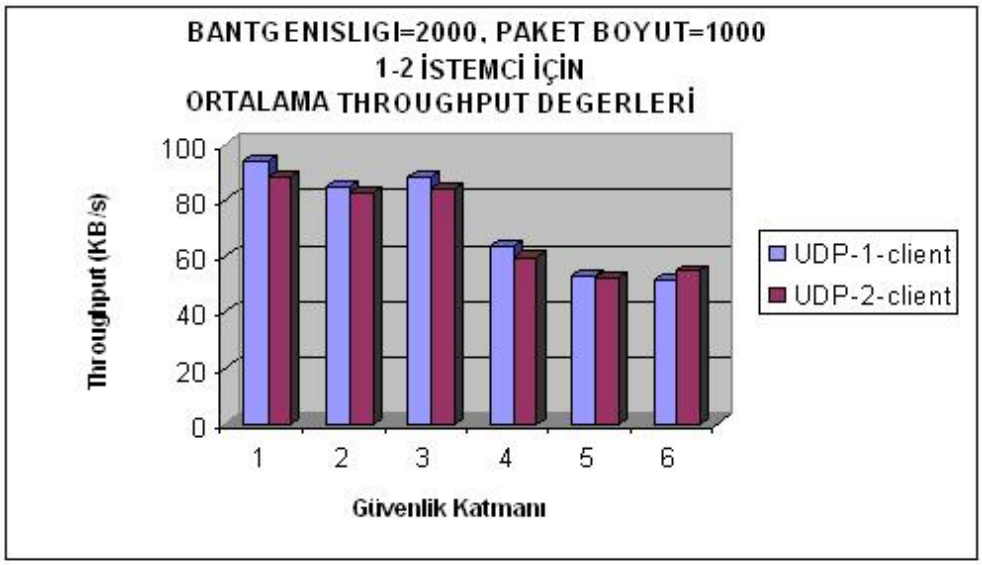
Tablo 4.15 : Güvenliksiz, 1 ve 2 istemcili ağlar için Throughput-Response Time değerleri

Security Layer	*Outgoing Bandwidth*	*Packet Length*	*# of client*	*TCP Throughput (Kbytes/sec)*	*TCP Response Time(sec)*
1	2000	Random	1	69,819	139,981
1	2000	Fix 100	1	72,036	68,983
1	2000	Fix 500	1	72,088	110,77
1	2000	Fix 1000	1	76,71	168,042
1	2000	Fix 1500	1	72,857	254,684
Security Layer	*Outgoing Bandwidth*	*Packet Length*	*# of client*	*TCP Throughput (Kbytes/sec)*	*TCP Response Time(sec)*
1	2000	Random	2	68,639	137,033
1	2000	Fix 100	2	69,459	67,731
1	2000	Fix 500	2	71,562	88,848
1	2000	Fix 1000	2	74,306	177,035
1	2000	Fix 1500	2	71,947	268,766

Sadece güvenlik olmayan sistemlerde değil, bütün güvenlik mekanizmaları için benzer karşılaştırma yapıldığında sistemde 1 istemci ile 2 istemci olması arasındaki fark oldukça düşüktür. Bütün güvenlik mekanizmaları için bu karşılaştırma sonucunda görülmüştür ki 2 istemcili sistemin throughput değeri , 1 istemcili sistemin %99.4'ü kadardır. Yani sistemde 2 istemci olduğunda , istemci başına düşen throughput % 49.7 değerine karşılık gelmektedir. Aşağıdaki grafiklerden de görüleceği gibi, sistemde istemci sayısı arttıkça toplam throughput değeri de azalmaktadır.



Şekil 4.23 : Tıkanıklık olmayan ağda, farklı güvenlik mekanizmaları için TCP 1client -2client için ortalama throughput değerleri

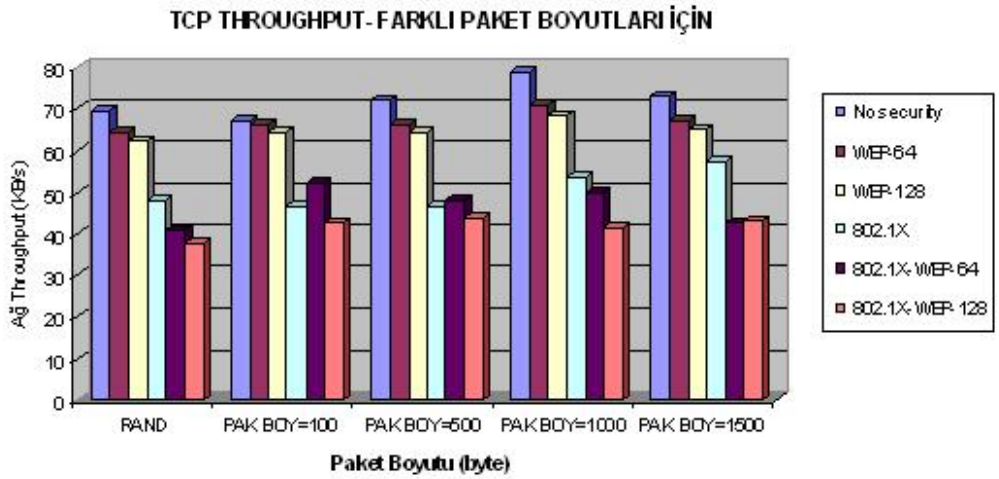


Şekil 4.23 : Tıkanıklık olmayan ağda, farklı güvenlik mekanizmaları için UDP 1client -2client için ortalama throughput değerleri

4.3.3. Paket boyutunun performansa etkisi

Tablo 4.16 : Farklı güvenlik mekanizmaları için değişen paket boyutlarının TCP throughput değerine etkisi

Security Layer	***Outgoing Bandwidth***	***Packet Length***	***# of client***	***TCP Throughput (Kbytes/sec)***	***TCP Response Time(sec)***
1	2000	Random	1	69,819	139,981
1	2000	Fix 100	1	72,036	68,983
1	2000	Fix 500	1	72,088	110,77
1	2000	Fix 1000	1	76,71	168,042
1	2000	Fix 1500	1	72,857	254,684
Security Layer	***Outgoing Bandwidth***	***Packet Length***	***# of client***	***TCP Throughput (Kbytes/sec)***	***TCP Response Time(sec)***
2	2000	Random	1	64,443	721,981
2	2000	Fix 100	1	66,489	408,923
2	2000	Fix 500	1	66,537	520,751
2	2000	Fix 1000	1	70,803	974,042
2	2000	Fix 1500	1	67,247	1004,672
Security Layer	***Outgoing Bandwidth***	***Packet Length***	***# of client***	***TCP Throughput (Kbytes/sec)***	***TCP Response Time(sec)***
5	2000	Random	1	40,773	746,528
5	2000	Fix 100	1	42,068	422,826
5	2000	Fix 500	1	42,098	538,457
5	2000	Fix 1000	1	44,797	1007,159
5	2000	Fix 1500	1	42,547	1038,831

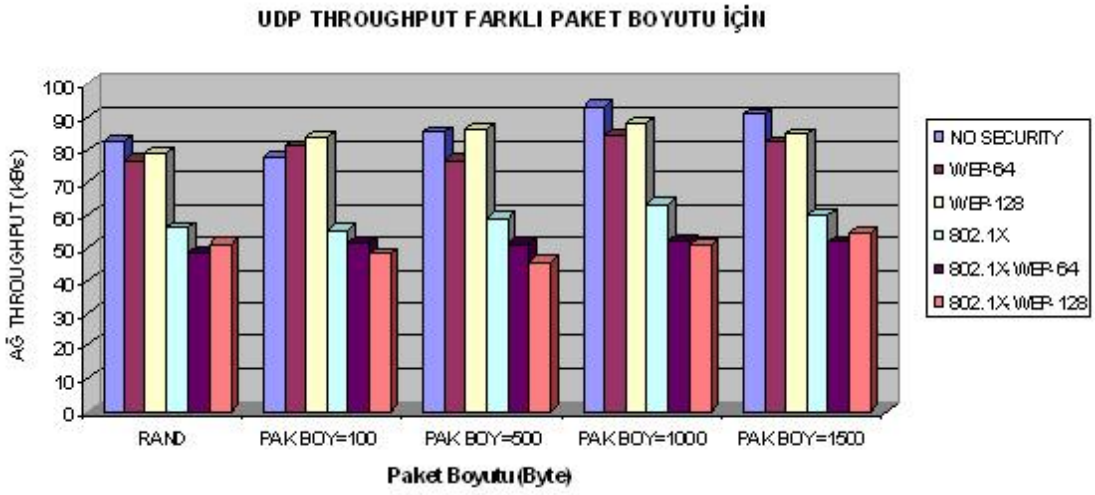


Şekil 4.24 : Farklı güvenlik mekanizmaları TCP Throughput değerine paket boyutunun etkisi

Yukarıdaki tablo ve grafiklerden görüldüğü gibi farklı güvenlik mekanizmaları incelendiğinde, TCP protokolünün kullanımında ve paket boyutunun 1000 olduğu deneylerde throughput değerleri kendi kategorisinde her zaman ilk sıradadır. Bununla beraber diğer değerlerin birbirlerine yakın oldukları ve farklı güvenlik mekanizmaları için birbirlerinden farklı sıralar aldıkları görülebilmektedir. EK-B 'deki bütün sonuçlar incelendiğinde de benzer sonuçlar görülebilmektedir.

Tablo 4.17 : Farklı güvenlik mekanizmaları için değişen paket boyutlarının UDP throughput değerine etkisi

Security Layer	***Outgoing Bandwidth***	***Packet Length***	***# of client***	***UDP Throughput (Kbytes/sec)***	***UDP Response Time(sec)***
1	2000	Random	1	82,871	130,01
1	2000	Fix 100	1	87,677	25,527
1	2000	Fix 500	1	87,367	87,2
1	2000	Fix 1000	1	89,132	170,979
1	2000	Fix 1500	1	88,83	285,51
Security Layer	***Outgoing Bandwidth***	***Packet Length***	***# of client***	***UDP Throughput (Kbytes/sec)***	***UDP Response Time(sec)***
2	2000	Random	1	76,556	195,15
2	2000	Fix 100	1	80,996	38,295
2	2000	Fix 500	1	80,710	127,54
2	2000	Fix 1000	1	82,340	256,467
2	2000	Fix 1500	1	82,061	428,21
Security Layer	***Outgoing Bandwidth***	***Packet Length***	***# of client***	***UDP Throughput (Kbytes/sec)***	***UDP Response Time(sec)***
5	2000	Random	1	48,446	198,350
5	2000	Fix 100	1	51,255	38,923
5	2000	Fix 500	1	51,074	129,632
5	2000	Fix 1000	1	52,106	260,673
5	2000	Fix 1500	1	51,929	435,233



Şekil 4.25 : Farklı güvenlik mekanizmaları UDP Throughput değerine paket boyutunun etkisi

Yukarıdaki tablo ve grafiklerden görüldüğü gibi farklı güvenlik mekanizmaları incelendiğinde, UDP protokolünün kullanımında ve paket boyutunun 1000 olduğu deneylerde throughput değerleri kendi kategorisinde her zaman ilk sıradadır. Bununla beraber diğer değerlerin birbirlerine yakın oldukları ve farklı güvenlik mekanizmaları için birbirlerinden farklı sıralar aldıkları görülebilmektedir. EK-B 'deki bütün sonuçlar incelendiğinde de benzer sonuçlar görülebilmektedir.

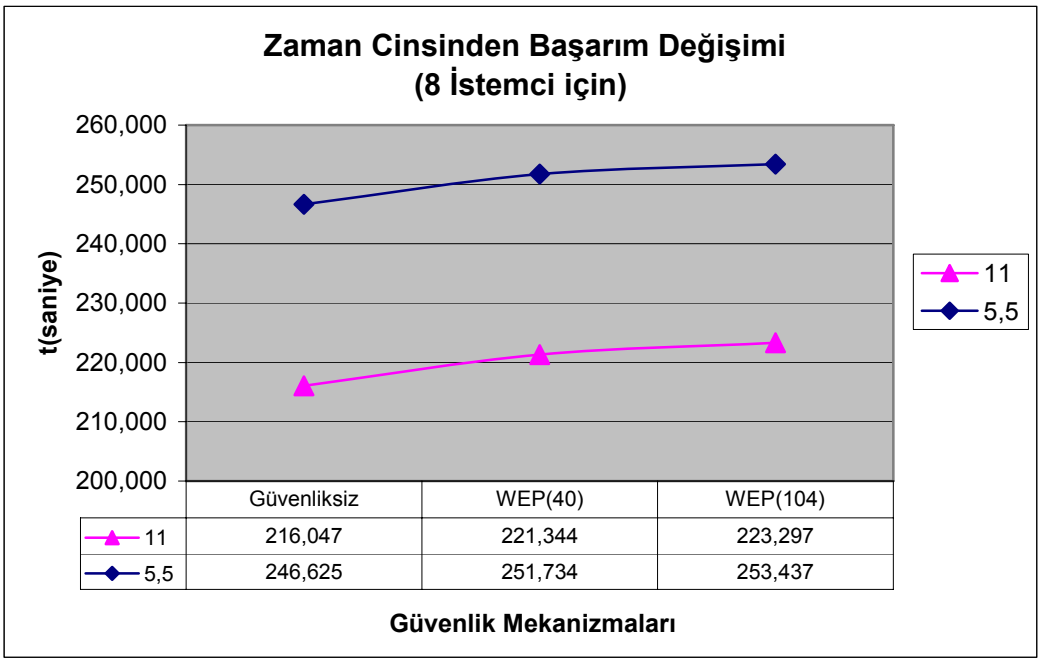
5. TARTIŞMA VE SONUÇ

İletişimin hava ortamında kontrolsüz bir şekilde gerçekleştiği kablosuz LAN sistemlerinde güvenliği sağlayabilmek için çeşitli güvenlik mekanizmaları geliştirilmiştir. Kablosuz LAN sistemleri için ilk nesil geliştirilen mekanizmaların açıklarının tespit edilmesi ile daha güvenli yöntemler geliştirilmiştir.

Bu çalışmada kablosuz LAN sistemleri için bugüne kadar geliştirilmiş güvenlik mekanizmalarının üzerinde durulmuştur. Çalışmanın ilk bölümünde bu mekanizmalar bir simülasyon çalışması ile gerçeklenerek güvenli sistemlerin performans başarımları elde edilmiştir. Çalışmanın ikinci kısmında ise bir erişim noktası ve kablosuz iletşim için gerekli donanıma sahip iki adet bilgisayar ile gerçek bir kablosuz ağ ortamında gerçekleştirilen deney çalışması yapılmıştır. Bu deney çalışmasında trafik üretmek ve ağ trafiğini toplanarak analiz edilmiştir. Baghaei [36] tarafından 802.11b ağlar için yapılan çalışmadan yola çıkılarak 802.11g ağ ortamında yeni sonuçlar elde edilmiştir.

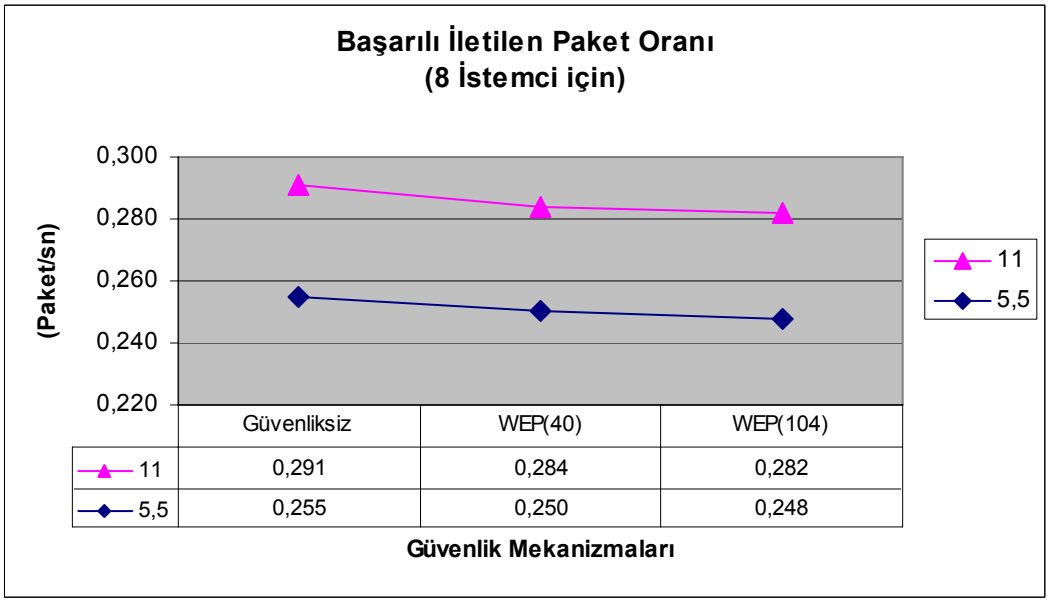
Öncelikle 802.11b, 802.11g ve 802.11i standartlarına uygun olarak çeşitli ağ topolojileri kullanılarak güvenlik mekanizmaları içermeyen sistemlerin performansı yapılan testler sonucu elde edilmiştir. Daha sonra ilk nesil güvenlik mekanizması olan WEP'in 802.11b ağlar üzerindeki etkisini incelemek üzere testler tekrarlanmıştır. WEP'in etkisini incelerken iki farklı anahtar uzunluğu ile çalışabilen WEP algoritması ayrı ayrı test edilmiştir. Bunlar 40 bit anahtar kullanan standart WEP ve 104 bit genişletilmiş anahtar kullanan WEP'tir.

Şekil 5.1'de de görüldüğü üzere ele aldığımız 8 istemcili ve güvenlik mekanizması içermeyen ağlarda sistemde iletim için geçen toplam süre güvenlik mekanizması içeren durumlara göre daha azdır. WEP'in ve arkaplanda kullandığı RC4 algoritmasının basit bir işleyişe sahip olmasından dolayı geçen toplam zamanlar arasında çok büyük farklılıklar bulunmamaktadır. Fakat anahtar uzunluğunun değişimi ile toplam zamanın arttığı göz önüne alınırsa güvenlik mekanizmasının var olmasının ve karmaşıklığının artmasının sistemin performans başarımını düşürdüğü görülmektedir.



Şekil 5.1 : Güvenli 802.11b (8 istemcili) ağların farklı veri hızları ile toplam geçen zaman değişimi

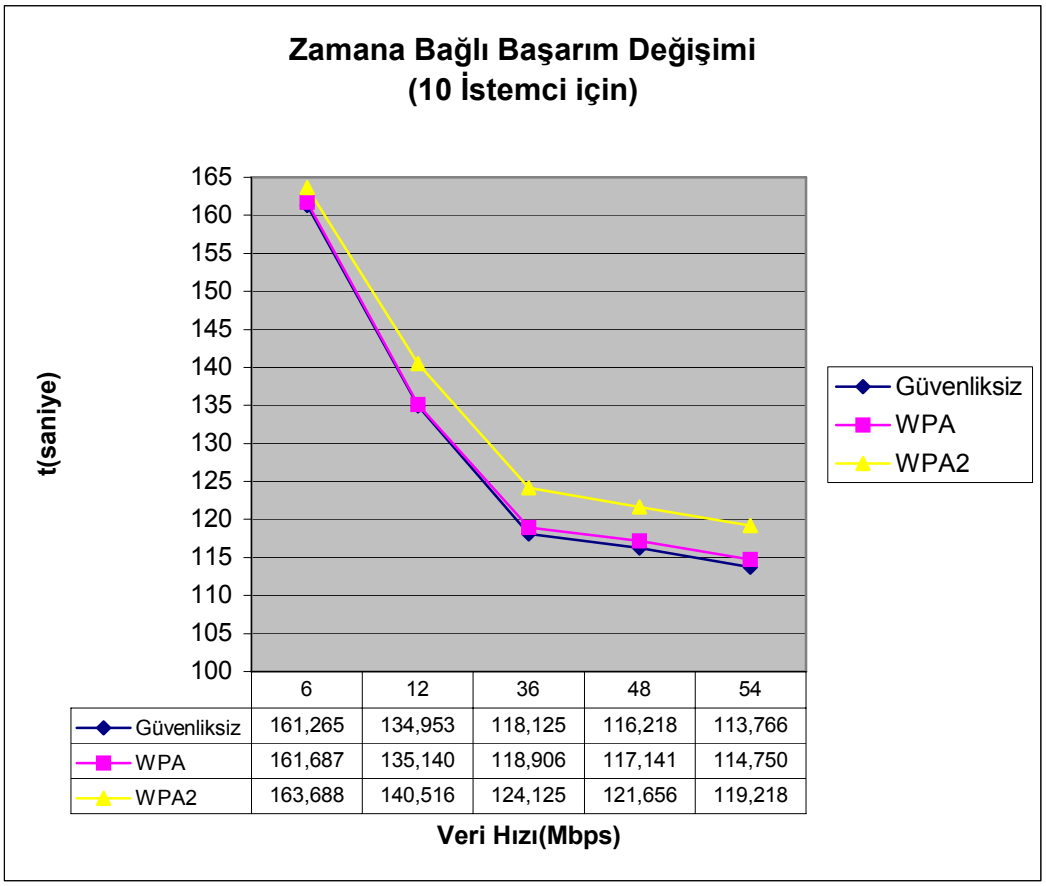
Şekil 5.2'de ise sistemde başarıyla hedefine ilertilen toplam paket sayısının zamana oranı yani yararlı yükün değişimi gözlenmektedir. Güvenlik mekanizmasının karmaşıklığının artması ile yararlı yükün düşüşü yani performans başarımında düşüş görülmüştür. Biri diğerinin iki katı olan veri hızlarının etkisi de sonuçlarda açıkça görülebilir. Veri hızı yüksek olan ağda toplam geçen zaman daha düşükken yararlı yük değeri daha yüksektir.



Şekil 5.2 : Güvenli 802.11b (8 istemcili) ağların farklı veri hızlarında yararlı yük değişimi

Bir diğer aşamada ise ikinci nesil güvenlik mekanizması olan WPA'nın ve güvenlik açısından köklü bir değişiklik getiren WPA'nin 802.11b ağlar üzerindeki etkisini incelemek üzere testler tekrarlanmıştır. Daha önce de bahsettiğimiz gibi 802.11i güvenlik için bir iyileştirme olduğu için 802.11g ağların fiziksel özelliklerini kullanarak test edilmiştir. Böylece aynı tip ağlar için uygun olan WPA ile karşılaştırılması sağlanmıştır.

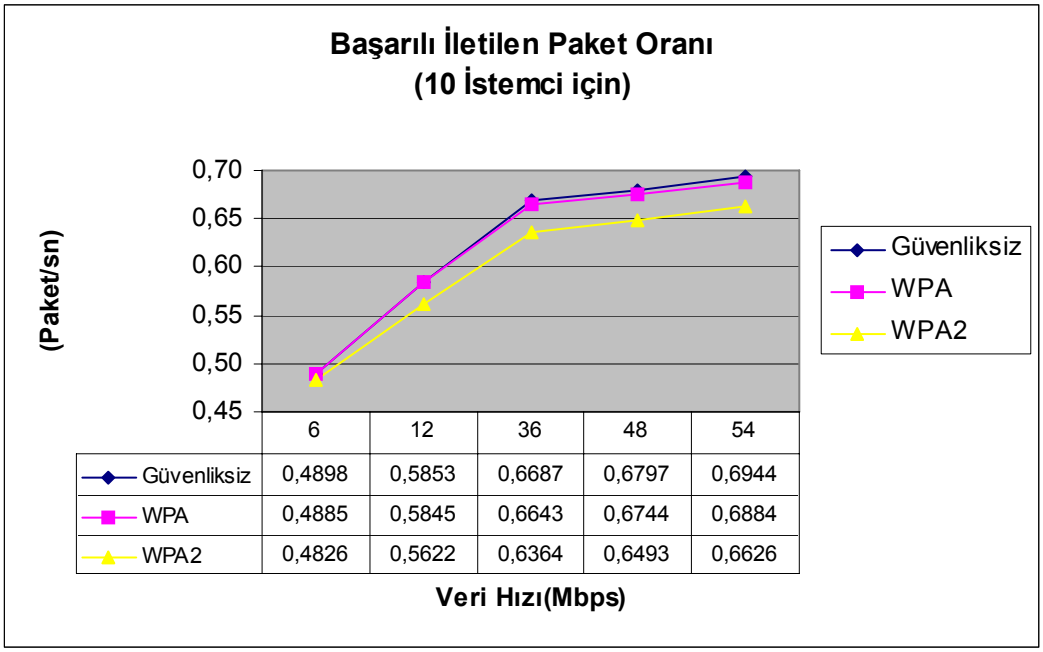
Şekil 5.3'de görüldüğü üzere 10 istemcili ve güvenlik mekanizması içermeyen ağlarda sistemde iletim için geçen toplam süre güvenlik mekanizması içeren durumlara göre daha azdır fakat güvenliksiz durumla WPA aradında çok büyük farklılıklar bulunmamaktadır. AES gibi oldukça karmaşık bir algoritmaya dayanan WPA2'de ise toplam zamanın gözle görülür şekilde arttığı belirlenmiştir. Bu değerlendirmede karmaşıklığın artmasının etkisi çok açık bir şekilde gözükmektedir. Ayrıca yine Şekil 5.3'ten görüldüğü gibi artan veri hızları ile iletim için geçen toplam zamanda belirgin düşüşler elde edilmiştir.



	6	12	36	48	54
Güvenliksiz	161,265	134,953	118,125	116,218	113,766
WPA	161,687	135,140	118,906	117,141	114,750
WPA2	163,688	140,516	124,125	121,656	119,218

Şekil 5.3 : Güvenli 802.11g (10 istemcili) ağların farklı veri hızları ile toplam geçen zaman değişimi

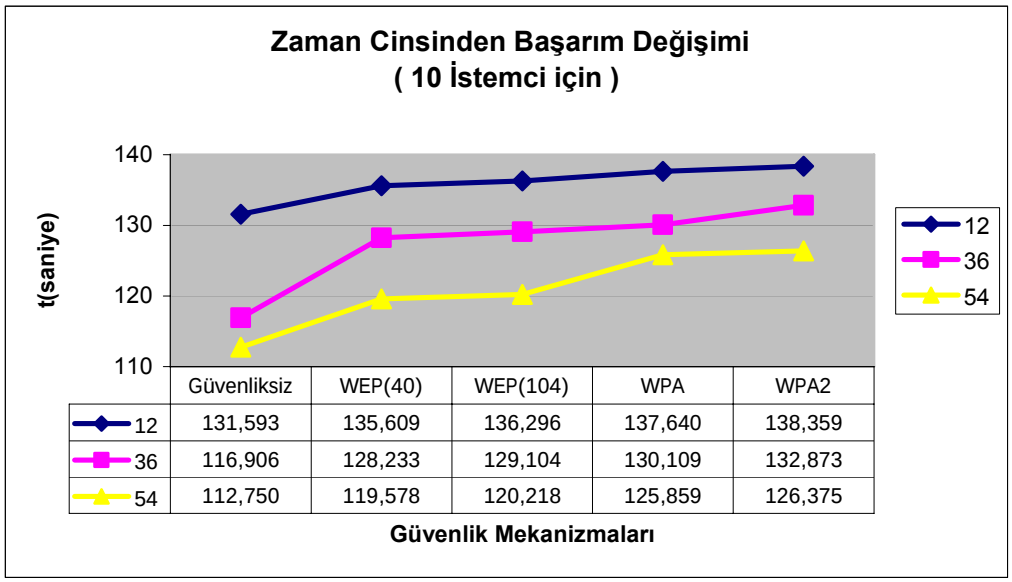
Şekil 5.4'de ise yine 10 istemcili 802.11g ağlarda başarıyla hedefine ilertilen toplam paket sayısının zamana oranı yani yararlı yükün değişimi gözlenmektedir. Güvenlik mekanizmasının karmaşıklığının artması ile yararlı yükün düşüşü yani performans başarımında düşüş görülmüştür. Farklı veri hızlarının etkisi de sonuçlarda açıkça görülebilir. Daha yüksek veri hızı daha başarılı bir iletim ortalamasını getirmiştir.



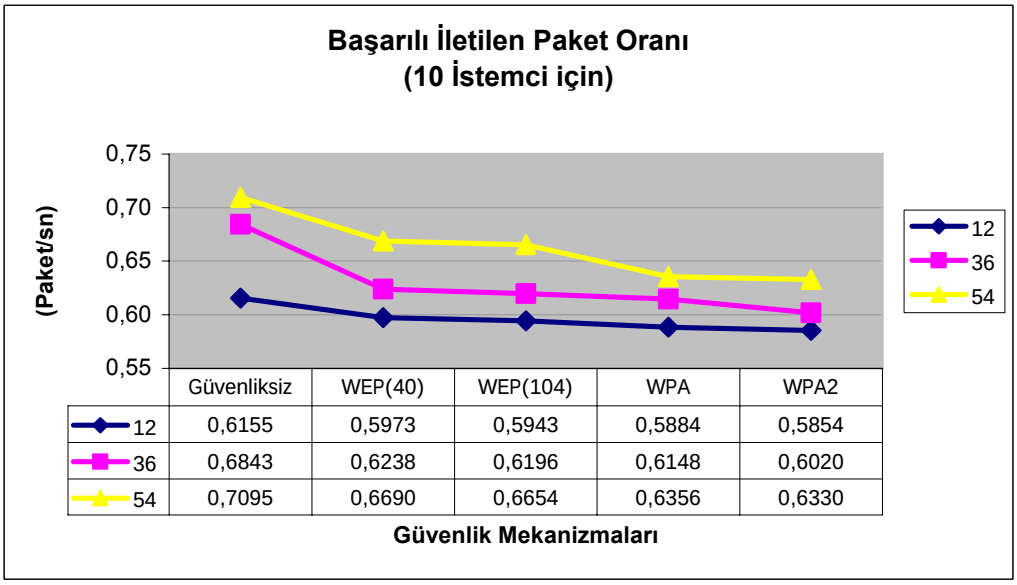
	6	12	36	48	54
Güvenliksiz	0,4898	0,5853	0,6687	0,6797	0,6944
WPA	0,4885	0,5845	0,6643	0,6744	0,6884
WPA2	0,4826	0,5622	0,6364	0,6493	0,6626

Şekil 5.4 : Güvenli 802.11g (10 istemcili) ağların farklı veri hızlarında yararlı yük değişimi

Simülasyon çalışmasında gerçekleştirilen testlerin büyük çoğunluğunda farklı güvenlik mekanizmalarının karşılaştırmak amacıyla paket boyutlarının dağılı sabit dağılım olarak seçilmiştir. Paket boyutlarının değişimi durumunda ağ performansında değişiklik olup olmadığını incelemek amacıyla üstel dağılım kullanılarak da testler gerçekleştirilmiştir. Büyük boyutlu 802.11g ağlar için gerçekleştirilen testlerden 10 istemci için elde edilen ortalama sonuçları Şekil 5.5 ve Şekil 5.6'da görülmektedir. Farklı veri hızlarını ifade eden eğrilerden görüldüğü gibi, sabit dağılım kadar düzgün olmasa da üstel dağılımın da toplam zaman ve yararlı yük oranı cinsinden benzer sonuçlar verdiği görülmüştür.



Şekil 5.5 : Güvenli 802.11g (10 istemcili) ağların farklı veri hızları ile toplam geçen zaman değişimi



Şekil 5.6: Güvenli 802.11g (10 istemcili) ağların farklı veri hızlarında yararlı yük değişimi

Yapılan deneysel çalışmanın sonuçları incelendiğinde ağ doyuma ulaşmamışken (tıkanıklık oluşmamışken) güvenlik mekanizmalarının karmaşıklığındaki artışın sistem performansını önemli ölçüde düşürdüğü gözlenmiştir. Sistem performansının düşmesi sistemdeki toplam yararlı yük miktarının azalması ve toplam geçen zamanın artışı şeklinde olmaktadır.

Ağda tıkanıklığın oluştuğu durumlarda ise WEP algoritmasını içeren 2-3-5-6 numaralı güvenlik mekanizmalarına sahip sistemlerde hem TCP hem de UDP için yararlı yük değerinin diğerlerinden daha düşük olduğu görülmektedir. Toplam geçen zaman (cevap süreleri) incelendiğinde de yararlı yüke benzeyen bir durum söz konusudur. WEP algoritmasını içeren güvenlik katmanının aktif olduğu yerlerde toplam sürenin daha fazla olduğu görülmektedir. Bu durumlarda WEP'in varlığının sistemi 802.1X 'den daha fazla etkilediği söylenebilir. Bununla birlikte istemci sayısının artması sistemin toplam yük değerini küçük bir oranda da olsa azaltmaktadır.

Deneysel çalışmanın sonuçlarını TCP ve UDP protokollerinin performansı açısından incelersek, TCP'nin performansının daha düşük olduğu görülmektedir. Bununla birlikte UDP'nin bağlantısız bir protokol olmasından dolayı tıkanıklık meydana gelen ağlarda daha fazla paketin düşmesine sebep olduğu da bir gerçektir.

Yapılan çalışmaların ortalama ve karakteristik özelliklerini veren değerlendirmelerden de görüleceği gibi gelişen ve karmaşıklığı artan güvenlik mekanizmaları kablosuz LAN sistemlerinde performansı düşürmektedir. Savunmasız ve denetimi zor olan hava ortamındaki iletimin gizliliğini sağlayabilmek için sistem performansındaki düşüş göze alınmak durumundadır.

KAYNAKLAR

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

2. Intel Exploring WLAN Solutions, *What is Wireless LAN Networking?* [online], http://www.intel.com/business/bss/infrastructure/wireless/solutions/index.htm

3. DUNNE, D., 2001, *What is a wireless LAN?* [online] http://www.cnn.com/2001/TECH/ptech/05/10/what.is.WLAN.idg/index.html

4. POLLIN, D.,MAXIM, M., 2002, Wireless Security, RSA Press, McGraw Hill.

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

6. HATAMBEIKI, A., 2004, Wireless Network Security, Thesis (MS), Master of Science In Engineering: Computer and Communications, San Francisco State University

7. HAMID, R. A., 2003, Wireless LAN: Security Issues and Solutions, GIAC Security Essentials Certification (GSEC) Practical Assignment Version 1.4b Option 1, SANS Institute.

8. "What is WLAN?" The Wireless Networking Industry's Information Source, 2002, [online] http://www.pulsewan.com/data101/wireless_lan_basics.htm

9. GAST, M.S. , 2002., *802.11 Wireless Networks: The Definitive Guide*, Sebastopol, O'Reilly & Associates

10. IEEE Std 802.11 TASK GROUP, 1999, *IEEE 802.11 Standards for Local and Metropolitan Area Networks: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, http:// standards.ieee.org/ getieee802/ download/ 802.11-1999.pdf

11. IEEE Std 802.11 TASK GROUP, 1999, *IEEE 802.11 Standards for Local and Metropolitan Area Networks: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - High-speed Physical Layer in the 5 GHz Band*, http://standards.ieee.org/getieee802/download/802.11a-1999.pdf

12. IEEE Std 802.11 TASK GROUP, 1999, *IEEE 802.11 Standards for Local and Metropolitan Area Networks: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Higher-Speed Physical Layer Extension in the 2.4 GHz Band*, http://standards.ieee.org/getieee802/download/802.11b-1999.pdf

13. IEEE Std 802.11 TASK GROUP, 2003, *IEEE 802.11 Standards for Local and Metropolitan Area Networks: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band*, http://standards.ieee.org/getieee802/download/802.11g-1999.pdf

14. KHAN, J., KHWAJA, A., 2003, *Building secure wireless networks with 802.11*, Wiley, Indianapolis, Ind., ISBN: 0471237159

15. ROSHAN, P., LEARY J., 2004, *802.11 Wireless LAN fundamentals*, Cisco, Indianapolis, Ind., ISBN: 1587050773

16. WEBOPEDIA, *Webopedia Online Dictionary for Computer and Internet Terms* [online], http://www.webopedia.com/

17. NETWORKWORLD.COM, *Network World Fusion* [online], http://www.nwfusion.com/index.html

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

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

20. WINGET, N., HOUSLEY, R., WAGNER, D., WALKER, J., 2003, *Security Flaws in 802.11 Data Link Protocols*, Communications of the ACM, Vol 46, No:5

21. FLUHRER, S., MANTIN, I., and SHAMIR, A., 2001, *Weaknesses in the key Schedule Algorithm of RC4*, Proceedings of the 4th Annual Workshop on SelectedAreas of Cryptography

22. STUBBLEFIELD, A., IOANNIDIS, J.,RUBIN, A., 2002*, Using the Fluhrer, Mantin and Shamir Attack to break WEP*, Proceedings of the 2002 Network and Distributed Systems Security Symposium, 17-22

23. WALKER, J., 2000, *Unsafe at Any Key Size: An Analysis of the WEP Encapsulation*, Intel Corporation, doc: IEEE 802.11-00/ 362, www.dis.org/wl/pdf/unsafe.pdf

24. BORISOV, N. , GOLDBERG, I. , WAGNER, D. , 2001, *Intercepting mobile communications: The insecurity of 802.11*, Proceedings of the International Conference on Mobile Computing and Networking, Syf 180-189

25. ARBAUGH, W., 2001, *An Inductive Chosen Plaintext Attack Against WEP/WEP*, IEEE Document 802.11-02/230, http://www.cs.umd.edu/~waa/attack/frame.htm

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

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

28. EATON, D., 2002, *Diving into the 802.11i Spec: A Tutorial* [online], http:// www.commsdesign.com/ design_library/ cd/hn/ OEG20021126S0003

29. CORBETT, C., 2002, *Security for 802.11 Wireless Networks*, Techical Report, Department of Electrical and Computer Engineering Georgia Institute of Technology

30. RSA Security, What is RC4?, http://www.rsasecurity.com/rsalabs/node.asp?id=2250

31. WIKIPEDIA ONLINE ENCYCLOPEDIA , Cyclic Redundancy Check [online], http://en.wikipedia.org/wiki/Cyclic_redundancy_check

32. FERGUSON, N., 2002, Michael *: an improved MIC for 802.11 WEP*, doc : IEEE 802.11-02/020r0

33. WALKER, J., 2002, *The Temporal Key Integrity Protocol (TKIP)*, 802.11 Security Series Articles Part II, Intel Corporation

34. HOUSLEY, R., 2001, *Temporal Key Hash*, RSA Laboratories, doc.:IEEE 802.11-01/550r3

35. WALKER, J., 2002, *AES-based Encapsulations of 802.11 Data*, 802.11 Security Series Articles Part III, Intel Corporation

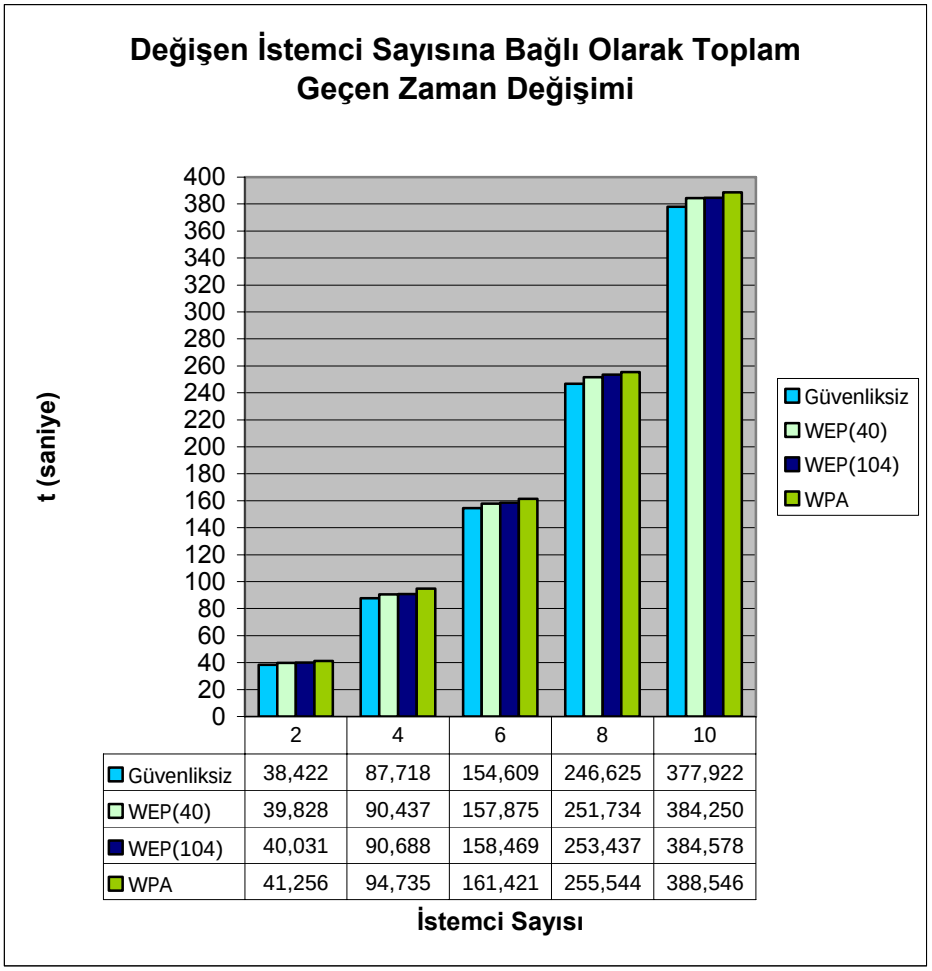
36. BAGHAEI, N., HUNT, R., Security performance of loaded IEEE 802.11b wireless networks, Computer Communications 27 (2004) 1746-1756, www.elsevier.com/locate/comcom

EK-A

SİMÜLASYON ÇALIŞMASINDAN ELDE EDİLEN TÜM SONUÇLAR

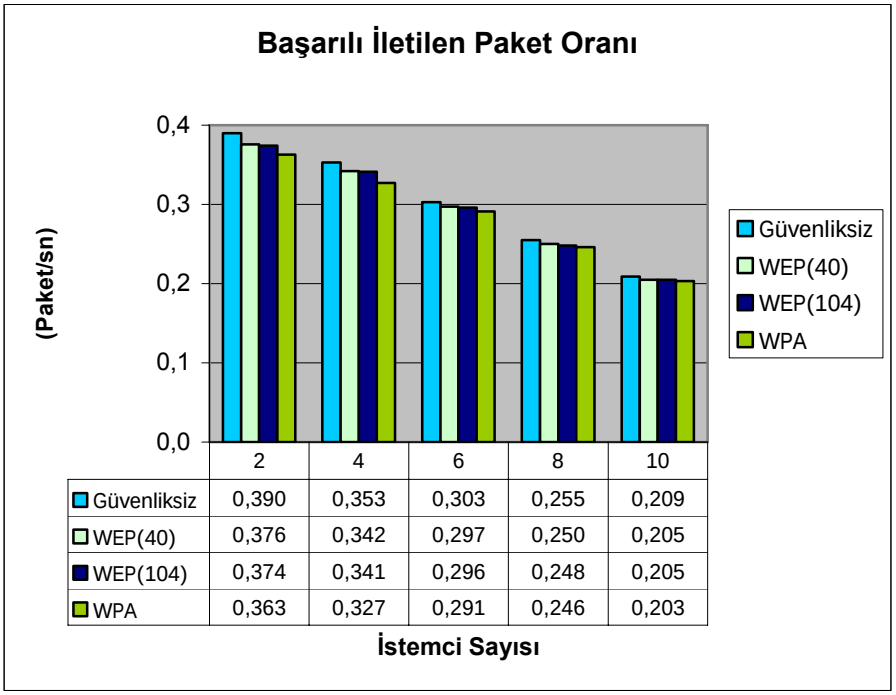
802.11b Ağlar için Sonuçlar

Bölüm 4.1.1.'de belirtilen giriş parametreleri ile yapılan testlerin 5.5 Mbps hızında çalışan küçük ve büyük boyutlu ağlar için elde edilen sonuç grafikleri aşağıda verilmektedir.



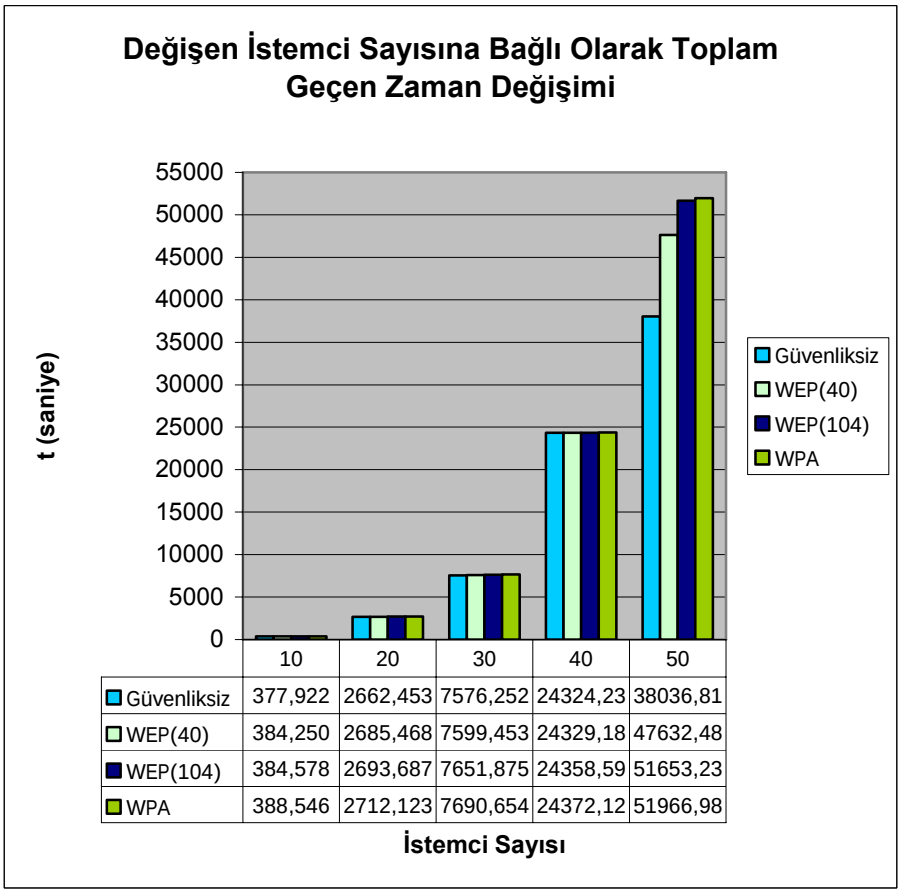
	2	4	6	8	10
Güvenliksiz	38,422	87,718	154,609	246,625	377,922
WEP(40)	39,828	90,437	157,875	251,734	384,250
WEP(104)	40,031	90,688	158,469	253,437	384,578
WPA	41,256	94,735	161,421	255,544	388,546

Şekil A.1 : Küçük boyutlu 802.11b (5,5 Mbps) Ağlar için Zaman Cinsinden Performans Değişimi



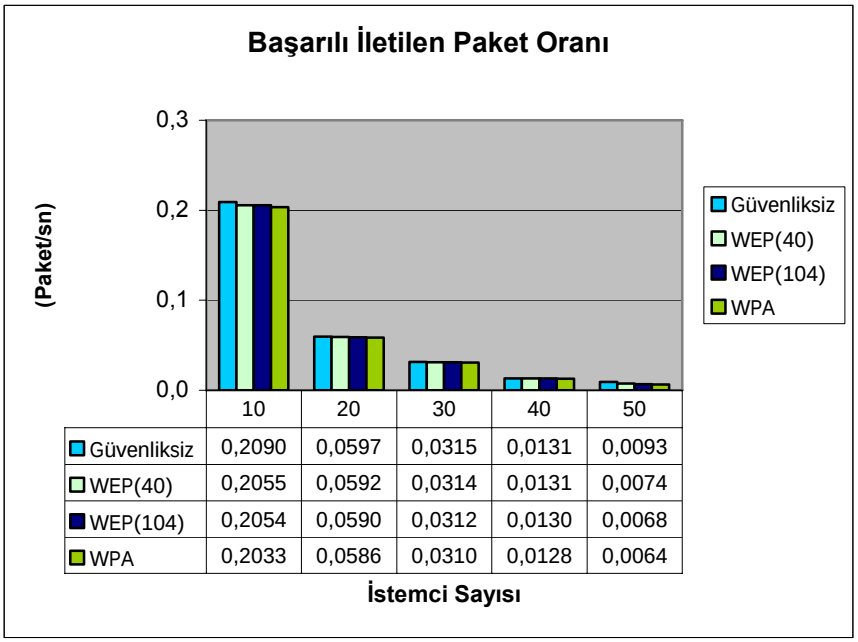
	2	4	6	8	10
Güvenliksiz	0,390	0,353	0,303	0,255	0,209
WEP(40)	0,376	0,342	0,297	0,250	0,205
WEP(104)	0,374	0,341	0,296	0,248	0,205
WPA	0,363	0,327	0,291	0,246	0,203

Şekil A.2 : Küçük boyutlu 802.11b (5,5 Mbps) Ağlar için Başarılı İletilen Paket Oranı



	10	20	30	40	50
Güvenliksiz	377,922	2662,453	7576,252	24324,23	38036,81
WEP(40)	384,250	2685,468	7599,453	24329,18	47632,48
WEP(104)	384,578	2693,687	7651,875	24358,59	51653,23
WPA	388,546	2712,123	7690,654	24372,12	51966,98

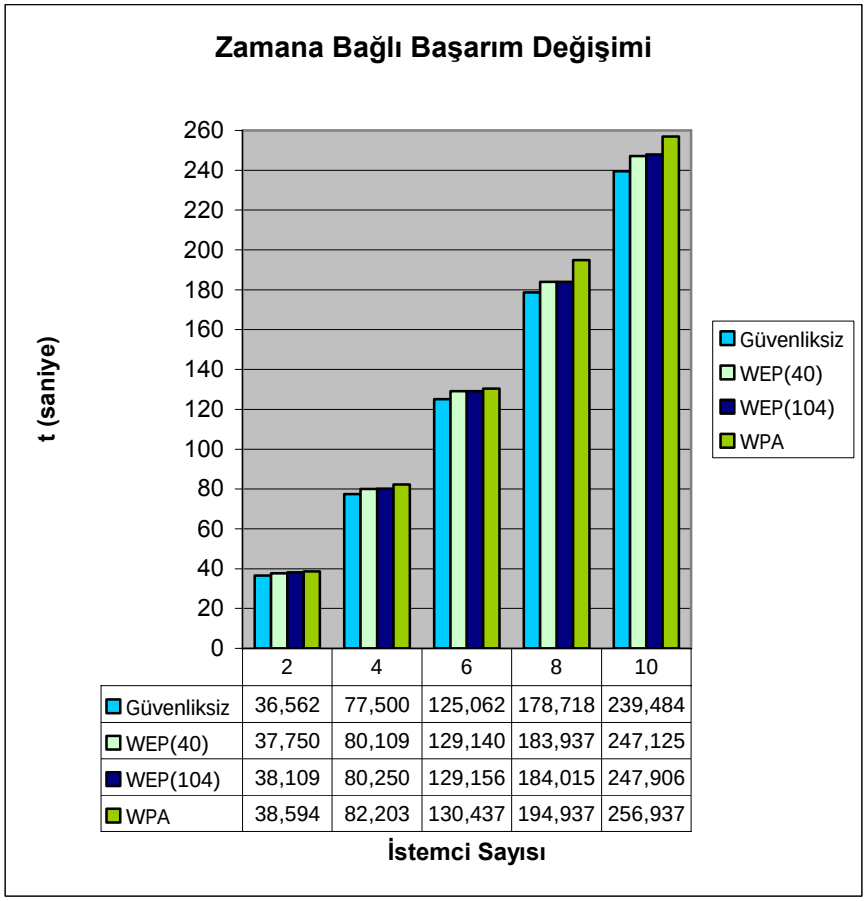
Şekil A.3 : Büyük boyutlu 802.11b (5,5 Mbps) Ağlar için Zaman Cinsinden Performans Değişimi



	10	20	30	40	50
Güvenliksiz	0,2090	0,0597	0,0315	0,0131	0,0093
WEP(40)	0,2055	0,0592	0,0314	0,0131	0,0074
WEP(104)	0,2054	0,0590	0,0312	0,0130	0,0068
WPA	0,2033	0,0586	0,0310	0,0128	0,0064

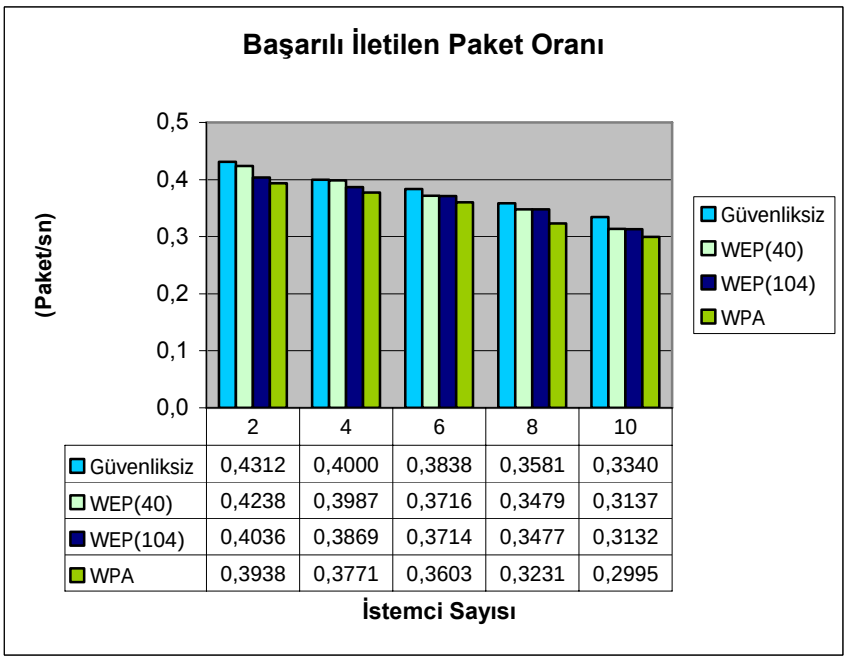
Şekil A.4 : Büyük boyutlu 802.11b (5,5 Mbps) Ağlar için Başarılı İletilen Paket Oranı

802.11b ağlar için yapılan testlerin büyük çoğunluğu sistemde koruma mekanizması olmadan gerçekleştirilmiştir. 11 Mbps hızında çalışan küçük boyutlu ağlar için RTS/CTS koruma mekanizması kullanılarak gerçekleştirilen testlerin sonuç grafikleri aşağıda gösterilmiştir.



	2	4	6	8	10
Güvenliksiz	36,562	77,500	125,062	178,718	239,484
WEP(40)	37,750	80,109	129,140	183,937	247,125
WEP(104)	38,109	80,250	129,156	184,015	247,906
WPA	38,594	82,203	130,437	194,937	256,937

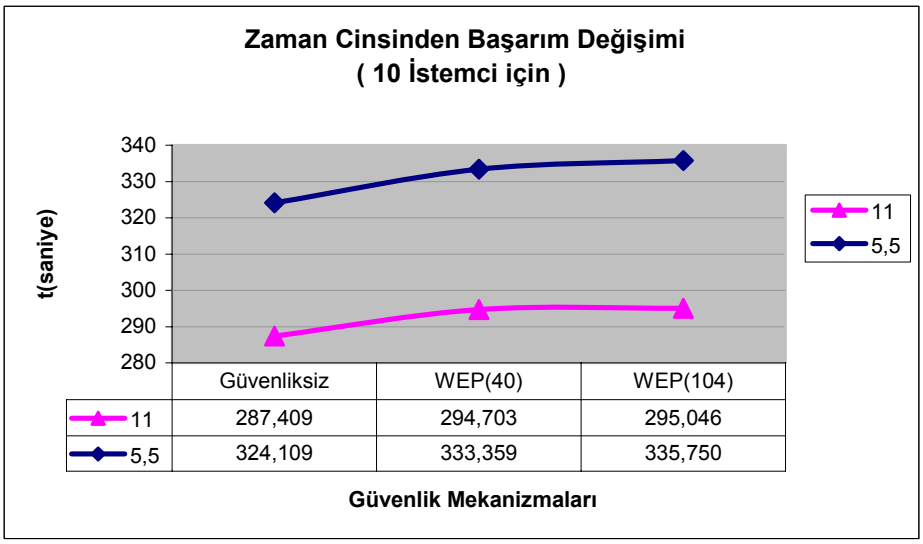
Şekil A.5 : RTS/CTS koruma mekanizması ile küçük boyutlu 802.11b (11 Mbps) ağlar için Zaman Cinsinden Performans Değişimi



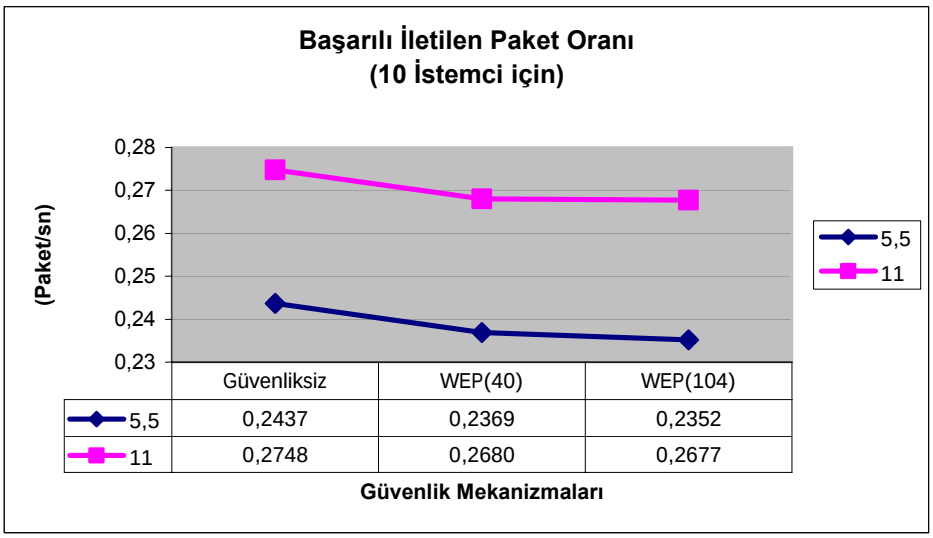
	2	4	6	8	10
Güvenliksiz	0,4312	0,4000	0,3838	0,3581	0,3340
WEP(40)	0,4238	0,3987	0,3716	0,3479	0,3137
WEP(104)	0,4036	0,3869	0,3714	0,3477	0,3132
WPA	0,3938	0,3771	0,3603	0,3231	0,2995

Şekil A.6 : RTS/CTS koruma mekanizması ile küçük boyutlu 802.11b (11 Mbps) ağlar için Başarılı İletilen Paket Oranı

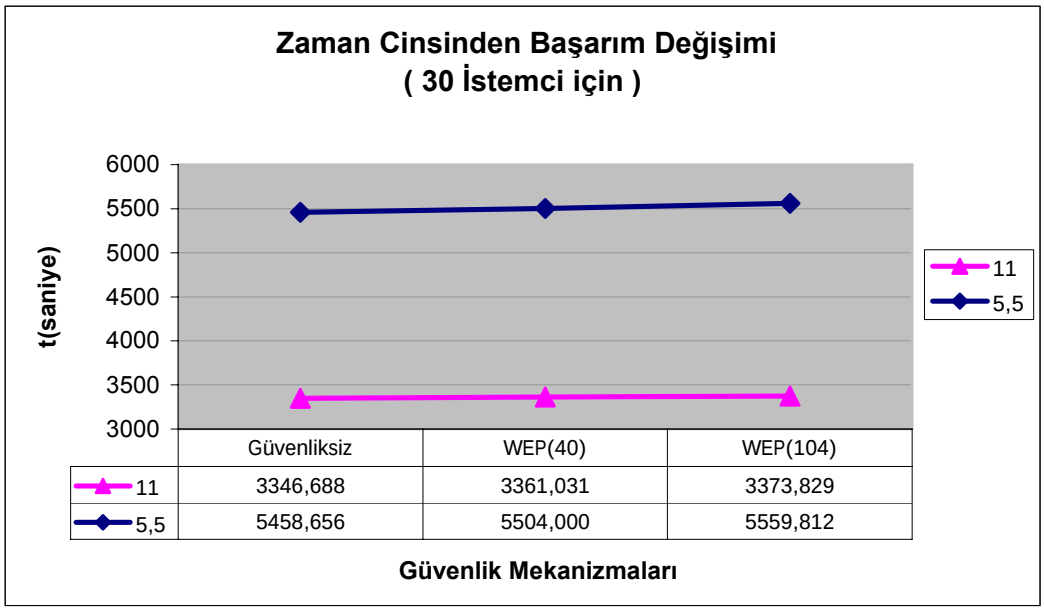
Bölüm 4.1.1.'de belirtilen giriş parametreleri ile yapılan testler paket boyutları sabit dağılım kullanılarak gerçekleştirilmiştir. Bu bölümde 5,5 ve 11 Mbps hızlarındaki büyük boyutlu 802.11b ağlarda paket boyutularının uniform dağılıma göre üretildiği simülasyon sonuçlarına yer verilmiştir. 10, 30 ve 50 istemcili ağlar için elde edilen sonuç grafikleri aşağıda verilmiştir.



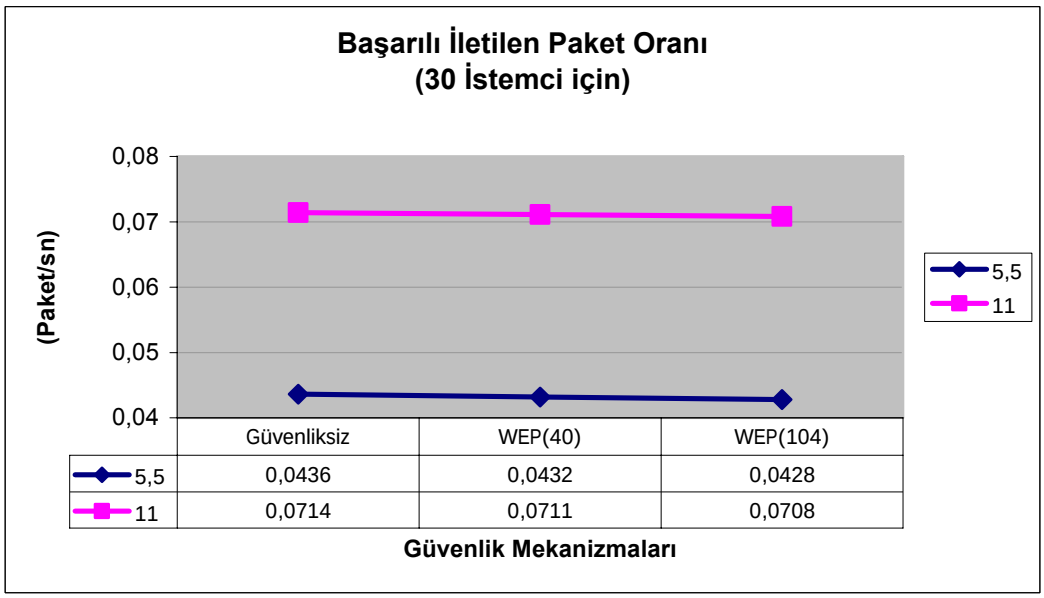
Şekil A.7 : Güvenli 802.11b (10 istemcili) ağların farklı veri hızları ile toplam geçen zaman değişimi



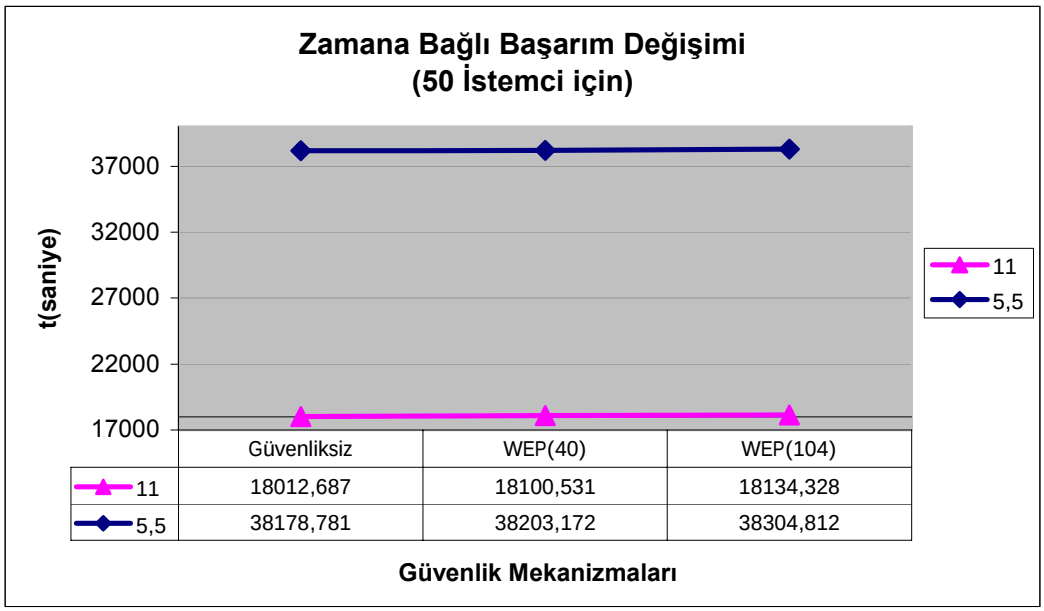
Şekil A.8 : Güvenli 802.11b (10 istemcili) ağların farklı veri hızlarında yararlı yük değişimi



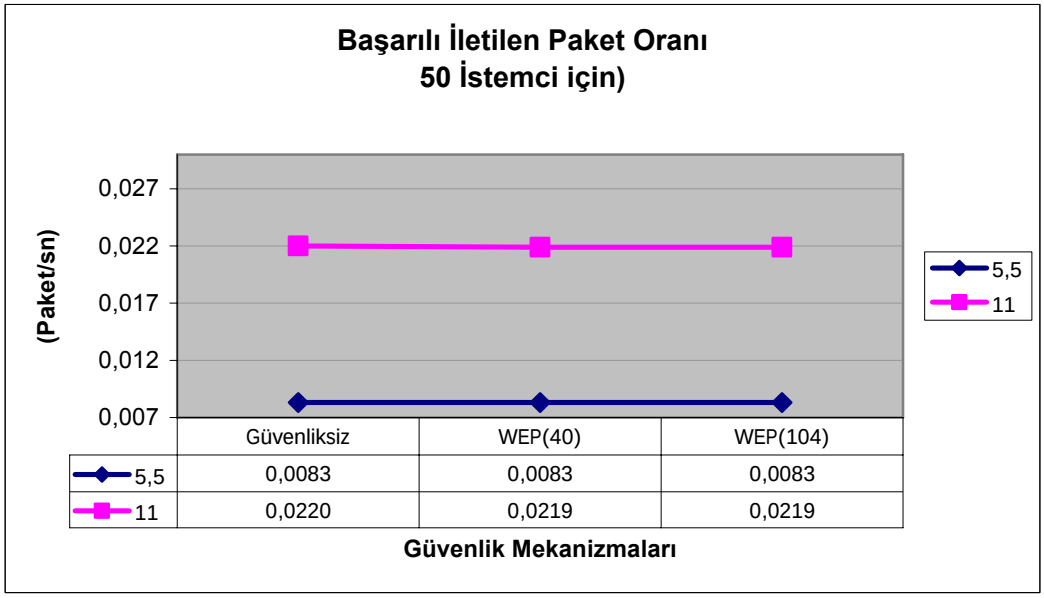
Şekil A.9 : Güvenli 802.11b (30 istemcili) ağların farklı veri hızları ile toplam geçen zaman değişimi



Şekil A.10 : Güvenli 802.11b (30 istemcili) ağların farklı veri hızlarında yararlı yük değişimi



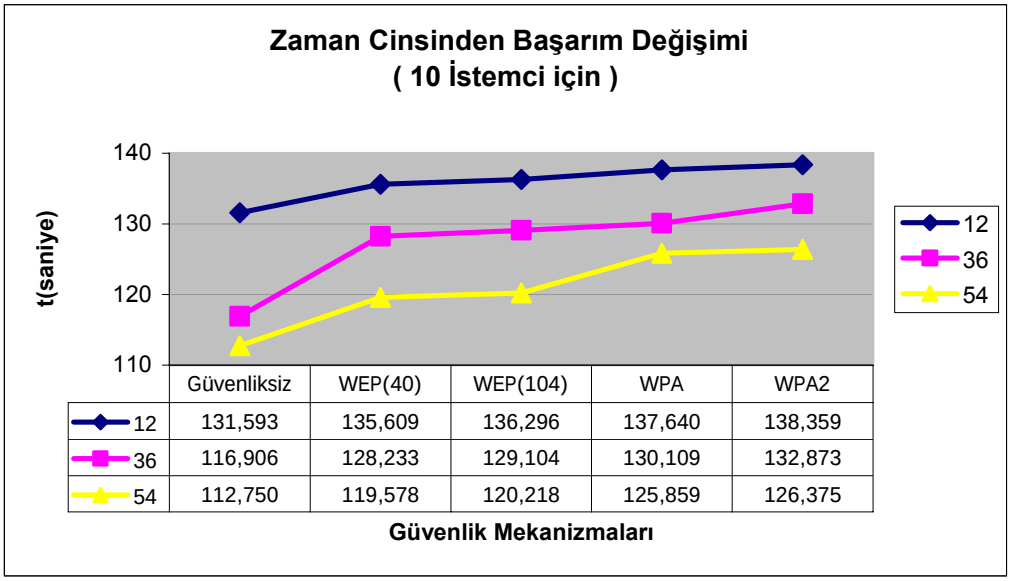
Şekil A.11 : Güvenli 802.11b (50 istemcili) ağların farklı veri hızları ile toplam geçen zaman değişimi



Şekil A.12 : Güvenli 802.11b (50 istemcili) ağların farklı veri hızlarında yararlı yük değişimi

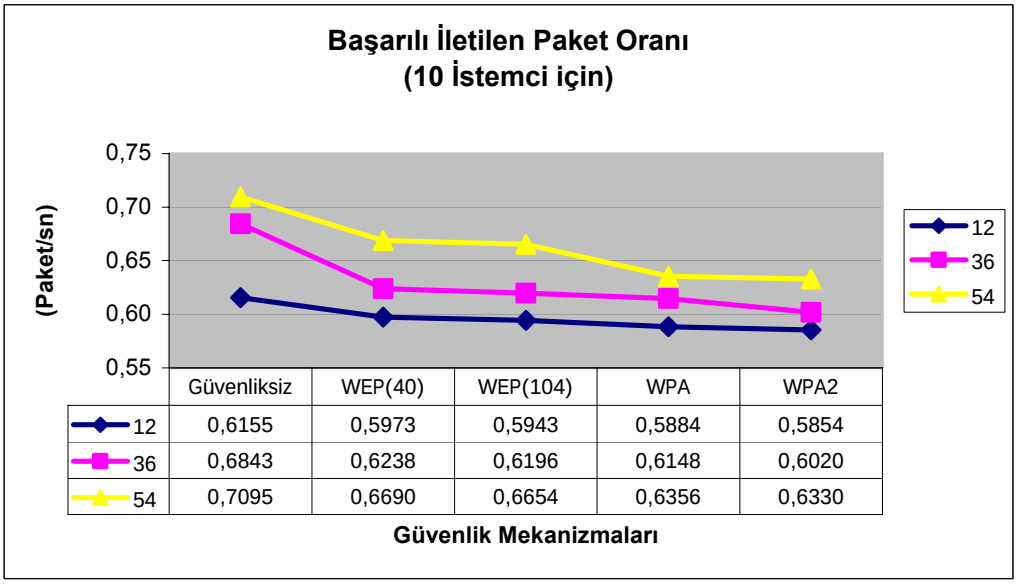
802.11g Ağlar için Sonuçlar

Bölüm 4.2.1.'de belirtilen giriş parametreleri ile yapılan testler paket boyutları sabit dağılım kullanılarak gerçekleştirilmiştir. Bu bölümde 12, 36 ve 54 Mbps hızlarındaki büyük boyutlu 802.11g ağlarda paket boyutularının üstel dağılıma göre üretildiği simülasyon sonuçlarına yer verilmiştir. 10, 30 ve 50 istemcili ağlar için elde edilen sonuç grafikleri aşağıda verilmiştir.



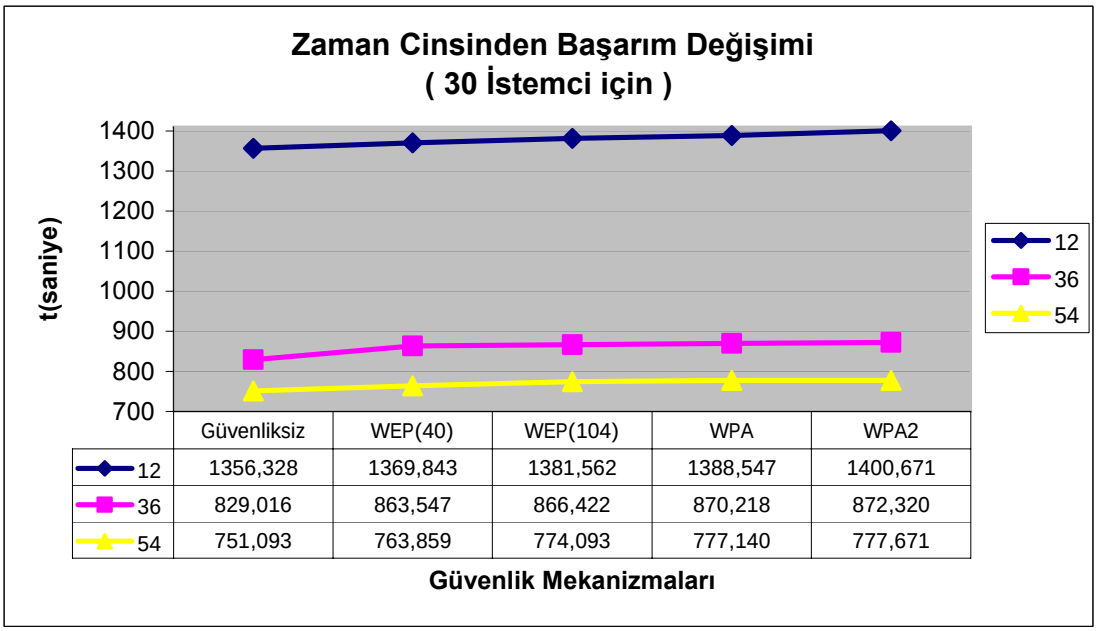
	Güvenliksiz	WEP(40)	WEP(104)	WPA	WPA2
12	131,593	135,609	136,296	137,640	138,359
36	116,906	128,233	129,104	130,109	132,873
54	112,750	119,578	120,218	125,859	126,375

Şekil A.13 : Güvenli 802.11g (10 istemcili) ağların farklı veri hızları ile toplam geçen zaman değişimi

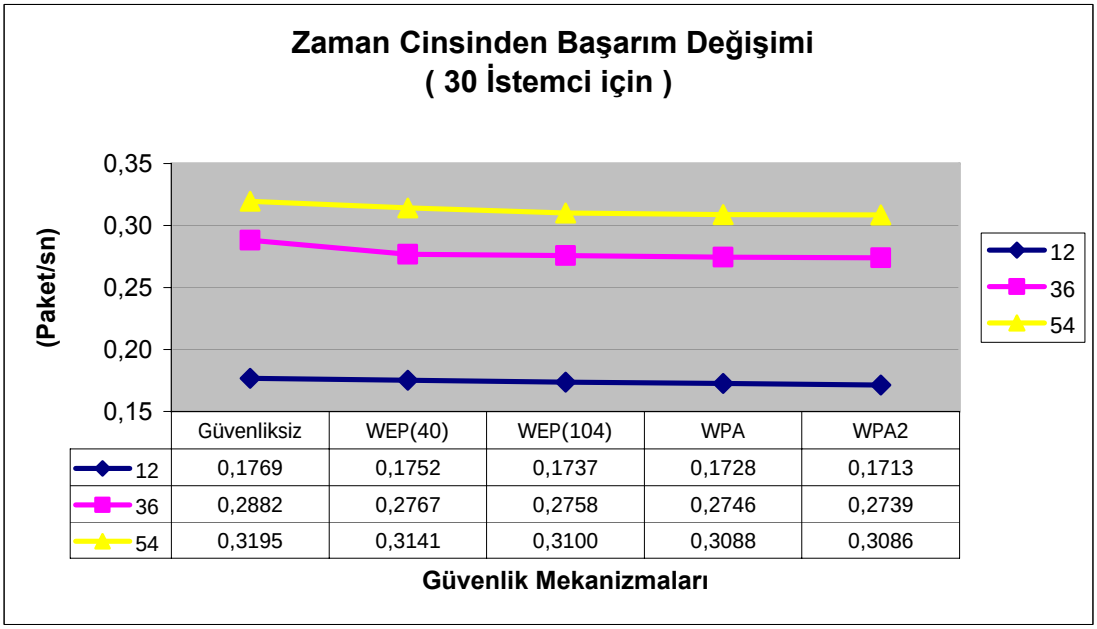


	Güvenliksiz	WEP(40)	WEP(104)	WPA	WPA2
12	0,6155	0,5973	0,5943	0,5884	0,5854
36	0,6843	0,6238	0,6196	0,6148	0,6020
54	0,7095	0,6690	0,6654	0,6356	0,6330

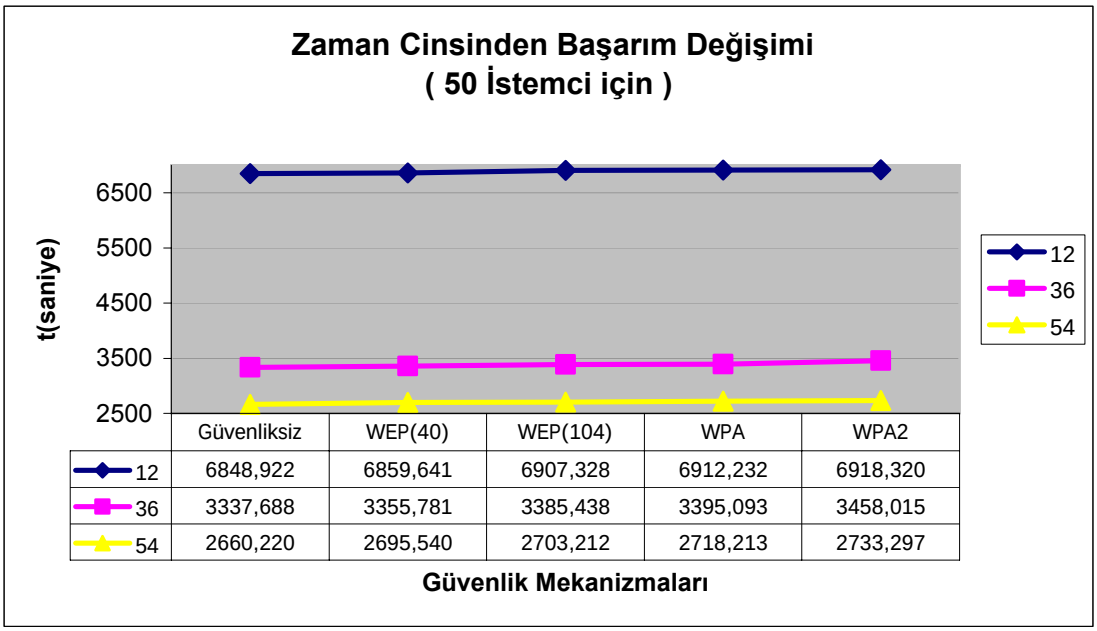
Şekil A.14 : Güvenli 802.11g (10 istemcili) ağların farklı veri hızlarında yararlı yük değişimi



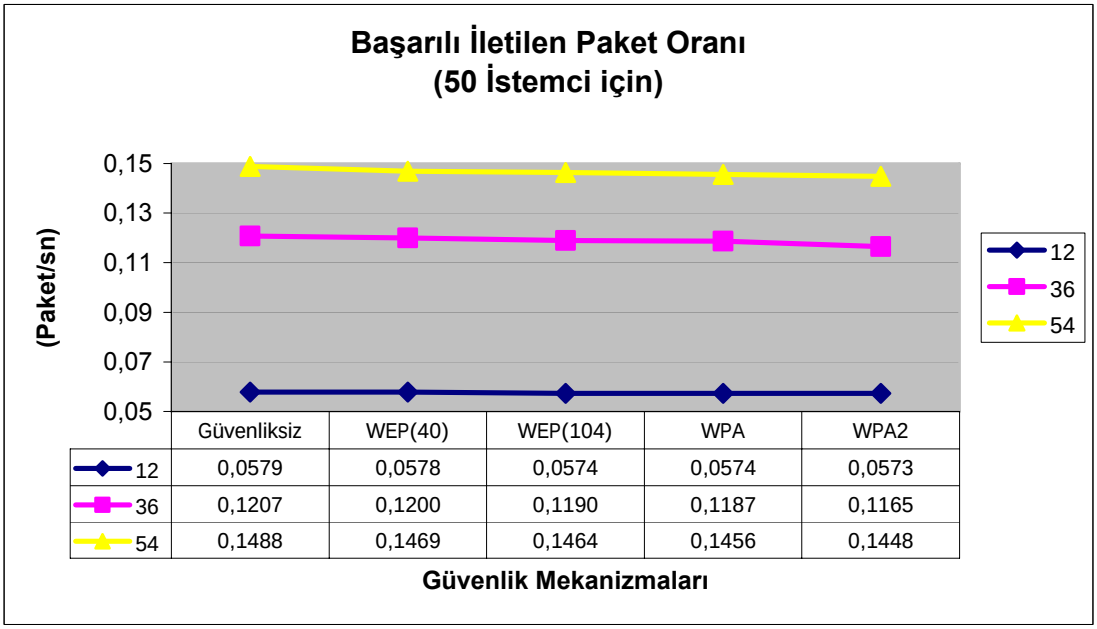
Şekil A.15 : Güvenli 802.11g (30 istemcili) ağların farklı veri hızları ile toplam geçen zaman değişimi



Şekil A.16 : Güvenli 802.11g (30 istemcili) ağların farklı veri hızlarında yararlı yük değişimi



Şekil A.17 : Güvenli 802.11g (50 istemcili) ağların farklı veri hızları ile toplam geçen zaman değişimi



Şekil A.18 : Güvenli 802.11g (50 istemcili) ağların farklı veri hızlarında yararlı yük değişimi

EK-B

DENEYSEL ÇALIŞMADAN ELDE EDİLEN TÜM SONUÇLAR

NO SECURITY - TCP

Security Layer	*Outgoing Bandwidth*	*Packet Length*	*# of clients*	*TCP Throughput (Kbytes/sec)*	*TCP Response Time(sec)*
1	**2000**	**Random**	**1**	**69,819**	**139,981**
1	**2000**	**Fix 100**	**1**	**72,036**	**68,983**
1	**2000**	**Fix 500**	**1**	**72,088**	**110,77**
1	**2000**	**Fix 1000**	**1**	**76,71**	**168,042**
1	**2000**	**Fix 1500**	**1**	**72,857**	**254,684**
1	25000	Random	**1**	1078,701	76,619
1	25000	Fix 100	**1**	1073,233	27,591
1	25000	Fix 500	**1**	1101,118	24,282
1	25000	Fix 1000	**1**	1221,593	22,992
1	25000	Fix 1500	**1**	1187,161	38,67
1	**55000**	**Random**	**1**	**1259,83**	**33,549**
1	**55000**	**Fix 100**	**1**	**1393,52**	**8,021**
1	**55000**	**Fix 500**	**1**	**1428,862**	**15,001**
1	**55000**	**Fix 1000**	**1**	**1605,161**	**22,005**
1	**55000**	**Fix 1500**	**1**	**1335,467**	**41,181**
1	**2000**	**Random**	**2**	**68,639**	**137,033**
1	**2000**	**Fix 100**	**2**	**69,459**	**67,731**
1	**2000**	**Fix 500**	**2**	**71,562**	**88,848**
1	**2000**	**Fix 1000**	**2**	**74,306**	**177,035**
1	**2000**	**Fix 1500**	**2**	**71,947**	**268,766**
1	25000	Random	**2**	1020,031	44,171
1	25000	Fix 100	**2**	1032,238	15,005
1	25000	Fix 500	**2**	1142,538	27,994
1	25000	Fix 1000	**2**	1256,54	31,123
1	25000	Fix 1500	**2**	1188,946	38,337
1	**55000**	**Random**	**2**	**1281,041**	**44,998**
1	**55000**	**Fix 100**	**2**	**1234,962**	**22,325**
1	**55000**	**Fix 500**	**2**	**1294,329**	**42,013**
1	**55000**	**Fix 1000**	**2**	**1408,835**	**63,008**
1	**55000**	**Fix 1500**	**2**	**1307,947**	**83,712**

NO SECURITY-UDP

Security Layer	*Outgoing Bandwidth*	*Packet Length*	*# of clients*	*UDP Throughput (Kbytes/sec)*	*UDP Response Time(sec)*
1	**2000**	**Random**	**1**	**82,871**	**130,01**
1	**2000**	**Fix 100**	**1**	**87,677**	**25,527**
1	**2000**	**Fix 500**	**1**	**87,367**	**87,2**
1	**2000**	**Fix 1000**	**1**	**89,132**	**170,979**
1	**2000**	**Fix 1500**	**1**	**88,83**	**285,51**
1	25000	Random	**1**	1378,65	25,613
1	25000	Fix 100	**1**	1273,532	17,557
1	25000	Fix 500	**1**	1320,252	22,857
1	25000	Fix 1000	**1**	1498,23	28,355
1	25000	Fix 1500	**1**	1321,432	40,235
1	**55000**	**Random**	**1**	**1559,83**	**33,549**
1	**55000**	**Fix 100**	**1**	**1408,63**	**17,526**
1	**55000**	**Fix 500**	**1**	**1431,31**	**22,125**
1	**55000**	**Fix 1000**	**1**	**1591,214**	**27,667**
1	**55000**	**Fix 1500**	**1**	**1507,672**	**45,437**
1	**2000**	**Random**	**2**	**81,821**	**147,99**
1	**2000**	**Fix 100**	**2**	**85,72**	**44,919**
1	**2000**	**Fix 500**	**2**	**85,367**	**86,881**
1	**2000**	**Fix 1000**	**2**	**88,132**	**190,672**
1	**2000**	**Fix 1500**	**2**	**87,83**	**335,018**
1	25000	Random	**2**	1279,652	52,743
1	25000	Fix 100	**2**	1221,015	28,989
1	25000	Fix 500	**2**	1390,671	33,513
1	25000	Fix 1000	**2**	1476,164	258,971
1	25000	Fix 1500	**2**	1471,124	74,003
1	**55000**	**Random**	**2**	**1399,83**	**34,552**
1	**55000**	**Fix 100**	**2**	**1302,63**	**18,526**
1	**55000**	**Fix 500**	**2**	**1331,31**	**23,129**
1	**55000**	**Fix 1000**	**2**	**1391,214**	**29,687**
1	**55000**	**Fix 1500**	**2**	**1307,672**	**48,523**

WEP 64 BIT-TCP

Security Layer	*Outgoing Bandwidth*	*Packet Length*	*# of clients*	*TCP Throughput (Kbytes/sec)*	*TCP Response Time(sec)*
2	**2000**	**Random**	**1**	**64,443**	**721,981**
2	**2000**	**Fix 100**	**1**	**66,489**	**408,923**
2	**2000**	**Fix 500**	**1**	**66,537**	**520,751**
2	**2000**	**Fix 1000**	**1**	**70,803**	**974,042**
2	**2000**	**Fix 1500**	**1**	**67,247**	**1004,672**
2	25000	Random	**1**	995,641	418,578
2	25000	Fix 100	**1**	990,594	157,268
2	25000	Fix 500	**1**	1016,332	138,412
2	25000	Fix 1000	**1**	1127,530	131,054
2	25000	Fix 1500	**1**	1095,750	220,134
2	**55000**	**Random**	**1**	**239,998**	**191,229**
2	**55000**	**Fix 100**	**1**	**265,466**	**45,719**
2	**55000**	**Fix 500**	**1**	**272,198**	**84,005**
2	**55000**	**Fix 1000**	**1**	**305,783**	**122,228**
2	**55000**	**Fix 1500**	**1**	**254,406**	**230,613**
2	**2000**	**Random**	**2**	**63,354**	**722,198**
2	**2000**	**Fix 100**	**2**	**64,111**	**406,382**
2	**2000**	**Fix 500**	**2**	**66,052**	**533,088**
2	**2000**	**Fix 1000**	**2**	**68,584**	**1062,32**
2	**2000**	**Fix 1500**	**2**	**66,407**	**1512,58**
2	25000	Random	**2**	941,489	265,02
2	25000	Fix 100	**2**	952,756	90,03
2	25000	Fix 500	**2**	1054,563	137,964
2	25000	Fix 1000	**2**	1159,786	198,738
2	25000	Fix 1500	**2**	1097,397	230,023
2	**55000**	**Random**	**2**	**266,668**	**267,998**
2	**55000**	**Fix 100**	**2**	**248,151**	**133,925**
2	**55000**	**Fix 500**	**2**	**253,615**	**251,178**
2	**55000**	**Fix 1000**	**2**	**265,026**	**328,048**
2	**55000**	**Fix 1500**	**2**	**249,112**	**502,272**

WEP 64 BIT-UDP

Security Layer	*Outgoing Bandwidth*	*Packet Length*	*# of clients*	*UDP Throughput (Kbytes/sec)*	*UDP Response Time(sec)*
2	**2000**	**Random**	**1**	**76,556**	**195,15**
2	**2000**	**Fix 100**	**1**	**80,996**	**38,295**
2	**2000**	**Fix 500**	**1**	**80,710**	**127,54**
2	**2000**	**Fix 1000**	**1**	**82,340**	**256,467**
2	**2000**	**Fix 1500**	**1**	**82,061**	**428,21**
2	25000	Random	**1**	1273,597	38,419
2	25000	Fix 100	**1**	1176,489	23,335
2	25000	Fix 500	**1**	1219,649	34,25
2	25000	Fix 1000	**1**	1384,065	41,52
2	25000	Fix 1500	**1**	1220,739	57,352
2	**55000**	**Random**	**1**	**709,013**	**50,323**
2	**55000**	**Fix 100**	**1**	**640,286**	**23,289**
2	**55000**	**Fix 500**	**1**	**650,595**	**35,187**
2	**55000**	**Fix 1000**	**1**	**723,278**	**41,502**
2	**55000**	**Fix 1500**	**1**	**685,305**	**62,156**
2	**2000**	**Random**	**2**	**76,732**	**221,985**
2	**2000**	**Fix 100**	**2**	**80,388**	**67,38**
2	**2000**	**Fix 500**	**2**	**80,057**	**120,633**
2	**2000**	**Fix 1000**	**2**	**82,650**	**266,94**
2	**2000**	**Fix 1500**	**2**	**82,367**	**469,052**
2	25000	Random	**2**	1200,058	73,841
2	25000	Fix 100	**2**	1145,068	40,585
2	25000	Fix 500	**2**	1304,171	46,919
2	25000	Fix 1000	**2**	1384,347	362,559
2	25000	Fix 1500	**2**	1379,620	102,604
2	**55000**	**Random**	**2**	**650,285**	**48,372**
2	**55000**	**Fix 100**	**2**	**605,132**	**25,953**
2	**55000**	**Fix 500**	**2**	**618,455**	**32,389**
2	**55000**	**Fix 1000**	**2**	**646,283**	**40,675**
2	**55000**	**Fix 1500**	**2**	**607,474**	**67,243**

WEP 128 BIT-TCP

Security Layer	*Outgoing Bandwidth*	*Packet Length*	*# of clients*	*TCP Throughput (Kbytes/sec)*	*TCP Response Time(sec)*
3	**2000**	**Random**	**1**	**62,286**	**779,76**
3	**2000**	**Fix 100**	**1**	**64,263**	**441,72**
3	**2000**	**Fix 500**	**1**	**64,310**	**562,68**
3	**2000**	**Fix 1000**	**1**	**68,433**	**1053,25**
3	**2000**	**Fix 1500**	**1**	**64,996**	**1085,45**
3	25000	Random	**1**	962,309	451,44
3	25000	Fix 100	**1**	957,431	170,64
3	25000	Fix 500	**1**	982,307	150,12
3	25000	Fix 1000	**1**	1089,783	142,56
3	25000	Fix 1500	**1**	1059,066	238,68
3	**55000**	**Random**	**1**	**240,010**	**207,36**
3	**55000**	**Fix 100**	**1**	**265,479**	**48,68**
3	**55000**	**Fix 500**	**1**	**272,212**	**90,72**
3	**55000**	**Fix 1000**	**1**	**305,799**	**131,76**
3	**55000**	**Fix 1500**	**1**	**254,420**	**248,45**
3	**2000**	**Random**	**2**	**61,235**	**779,765**
3	**2000**	**Fix 100**	**2**	**61,966**	**439,56**
3	**2000**	**Fix 500**	**2**	**63,843**	**575,735**
3	**2000**	**Fix 1000**	**2**	**66,291**	**1148,04**
3	**2000**	**Fix 1500**	**2**	**64,186**	**1632,96**
3	25000	Random	**2**	910,000	286,254
3	25000	Fix 100	**2**	920,890	98,285
3	25000	Fix 500	**2**	1019,292	149,045
3	25000	Fix 1000	**2**	1120,997	214,855
3	25000	Fix 1500	**2**	1060,694	249,458
3	**55000**	**Random**	**2**	**244,054**	**289,445**
3	**55000**	**Fix 100**	**2**	**235,276**	**144,648**
3	**55000**	**Fix 500**	**2**	**246,586**	**272,163**
3	**55000**	**Fix 1000**	**2**	**268,400**	**354,24**
3	**55000**	**Fix 1500**	**2**	**249,180**	**542,169**

WEP 128 BIT-UDP

Security Layer	*Outgoing Bandwidth*	*Packet Length*	*# of clients*	*UDP Throughput (Kbytes/sec)*	*UDP Response Time(sec)*
3	**2000**	**Random**	**1**	**79,069**	**194,152**
3	**2000**	**Fix 100**	**1**	**83,655**	**36,215**
3	**2000**	**Fix 500**	**1**	**83,359**	**123,154**
3	**2000**	**Fix 1000**	**1**	**85,043**	**246,447**
3	**2000**	**Fix 1500**	**1**	**84,755**	**438,139**
3	25000	Random	**1**	1315,402	38,325
3	25000	Fix 100	**1**	1215,106	21,355
3	25000	Fix 500	**1**	1259,683	36,125
3	25000	Fix 1000	**1**	1429,496	44,652
3	25000	Fix 1500	**1**	1260,809	59,322
3	**55000**	**Random**	**1**	**709,172**	**51,123**
3	**55000**	**Fix 100**	**1**	**640,430**	**22,389**
3	**55000**	**Fix 500**	**1**	**650,741**	**33,198**
3	**55000**	**Fix 1000**	**1**	**723,441**	**44,562**
3	**55000**	**Fix 1500**	**1**	**685,459**	**66,236**
3	**2000**	**Random**	**2**	**78,067**	**223,902**
3	**2000**	**Fix 100**	**2**	**81,788**	**65,213**
3	**2000**	**Fix 500**	**2**	**81,451**	**123,456**
3	**2000**	**Fix 1000**	**2**	**84,089**	**264,923**
3	**2000**	**Fix 1500**	**2**	**83,801**	**467,253**
3	25000	Random	**2**	1220,947	78,981
3	25000	Fix 100	**2**	1165,000	44,255
3	25000	Fix 500	**2**	1326,873	47,219
3	25000	Fix 1000	**2**	1408,444	363,659
3	25000	Fix 1500	**2**	1403,635	112,624
3	**55000**	**Random**	**2**	**629,287**	**49,472**
3	**55000**	**Fix 100**	**2**	**585,591**	**26,353**
3	**55000**	**Fix 500**	**2**	**598,484**	**33,329**
3	**55000**	**Fix 1000**	**2**	**625,413**	**42,256**
3	**55000**	**Fix 1500**	**2**	**587,857**	**68,223**

EAP-TLS (RADIUS SERVER) –TCP

Security Layer	*Outgoing Bandwidth*	*Packet Length*	*# of clients*	*TCP Throughput (Kbytes/sec)*	*TCP Response Time(sec)*
4	**2000**	**Random**	**1**	**45,088**	**139,981**
4	**2000**	**Fix 100**	**1**	**46,520**	**68,983**
4	**2000**	**Fix 500**	**1**	**46,554**	**110,77**
4	**2000**	**Fix 1000**	**1**	**49,539**	**168,042**
4	**2000**	**Fix 1500**	**1**	**47,050**	**254,684**
4	25000	Random	**1**	696,614	76,619
4	25000	Fix 100	**1**	693,083	27,591
4	25000	Fix 500	**1**	711,091	24,282
4	25000	Fix 1000	**1**	788,893	22,992
4	25000	Fix 1500	**1**	766,657	38,67
4	**55000**	**Random**	**1**	**1349,139**	**33,549**
4	**55000**	**Fix 100**	**1**	**1492,307**	**8,021**
4	**55000**	**Fix 500**	**1**	**1530,154**	**15,001**
4	**55000**	**Fix 1000**	**1**	**1718,951**	**22,005**
4	**55000**	**Fix 1500**	**1**	**1430,138**	**41,181**
4	**2000**	**Random**	**2**	**44,339**	**137,033**
4	**2000**	**Fix 100**	**2**	**44,869**	**67,731**
4	**2000**	**Fix 500**	**2**	**46,228**	**88,848**
4	**2000**	**Fix 1000**	**2**	**48,000**	**177,035**
4	**2000**	**Fix 1500**	**2**	**46,476**	**268,766**
4	25000	Random	**2**	658,920	44,171
4	25000	Fix 100	**2**	666,805	15,005
4	25000	Fix 500	**2**	738,057	27,994
4	25000	Fix 1000	**2**	811,700	31,123
4	25000	Fix 1500	**2**	768,035	38,337
4	**55000**	**Random**	**2**	**1383,242**	**44,998**
4	**55000**	**Fix 100**	**2**	**1333,487**	**22,325**
4	**55000**	**Fix 500**	**2**	**1397,591**	**42,013**
4	**55000**	**Fix 1000**	**2**	**1521,232**	**63,008**
4	**55000**	**Fix 1500**	**2**	**1412,295**	**83,712**

EAP-TLS (RADIUS SERVER) –UDP

Security Layer	*Outgoing Bandwidth*	*Packet Length*	*# of clients*	*UDP Throughput (Kbytes/sec)*	*UDP Response Time(sec)*
4	**2000**	**Random**	**1**	**56,012**	**130,01**
4	**2000**	**Fix 100**	**1**	**59,260**	**25,527**
4	**2000**	**Fix 500**	**1**	**59,050**	**87,2**
4	**2000**	**Fix 1000**	**1**	**60,243**	**170,979**
4	**2000**	**Fix 1500**	**1**	**60,039**	**285,51**
4	25000	Random	**1**	**931,816**	25,613
4	25000	Fix 100	**1**	**860,768**	17,557
4	25000	Fix 500	**1**	**892,345**	22,857
4	25000	Fix 1000	**1**	**1012,639**	28,355
4	25000	Fix 1500	**1**	**893,143**	40,235
4	**55000**	**Random**	**1**	**709,014**	**33,549**
4	**55000**	**Fix 100**	**1**	**640,286**	**17,526**
4	**55000**	**Fix 500**	**1**	**650,595**	**22,125**
4	**55000**	**Fix 1000**	**1**	**723,279**	**27,667**
4	**55000**	**Fix 1500**	**1**	**685,305**	**45,437**
4	**2000**	**Random**	**2**	**55,302**	147,99
4	**2000**	**Fix 100**	**2**	**57,937**	44,919
4	**2000**	**Fix 500**	**2**	**57,699**	86,881
4	**2000**	**Fix 1000**	**2**	**59,568**	190,672
4	**2000**	**Fix 1500**	**2**	**59,363**	335,018
4	25000	Random	**2**	**864,904**	52,743
4	25000	Fix 100	**2**	**825,272**	28,989
4	25000	Fix 500	**2**	**939,941**	33,513
4	25000	Fix 1000	**2**	**997,724**	258,971
4	25000	Fix 1500	**2**	**994,318**	74,003
4	**55000**	**Random**	**2**	**629,160**	**34,552**
4	**55000**	**Fix 100**	**2**	**585,473**	**18,526**
4	**55000**	**Fix 500**	**2**	**598,363**	**23,129**
4	**55000**	**Fix 1000**	**2**	**625,287**	**29,687**
4	**55000**	**Fix 1500**	**2**	**587,739**	**48,523**

EAP-TLS (RADIUS SERVER) -WEP 64 BIT –TCP

Security Layer	*Outgoing Bandwidth*	*Packet Length*	*# of clients*	*TCP Throughput (Kbytes/sec)*	*TCP Response Time(sec)*
5	**2000**	**Random**	**1**	**40,773**	**746,528**
5	**2000**	**Fix 100**	**1**	**42,068**	**422,826**
5	**2000**	**Fix 500**	**1**	**42,098**	**538,457**
5	**2000**	**Fix 1000**	**1**	**44,797**	**1007,159**
5	**2000**	**Fix 1500**	**1**	**42,547**	**1038,831**
5	25000	Random	**1**	629,940	432,810
5	25000	Fix 100	**1**	626,747	162,615
5	25000	Fix 500	**1**	643,031	143,118
5	25000	Fix 1000	**1**	713,386	135,510
5	25000	Fix 1500	**1**	693,278	227,619
5	**55000**	**Random**	**1**	**239,995**	**197,731**
5	**55000**	**Fix 100**	**1**	**265,463**	**47,273**
5	**55000**	**Fix 500**	**1**	**272,195**	**86,861**
5	**55000**	**Fix 1000**	**1**	**305,780**	**126,384**
5	**55000**	**Fix 1500**	**1**	**254,404**	**238,454**
5	**2000**	**Random**	**2**	40,084	**746,753**
5	**2000**	**Fix 100**	**2**	40,563	**420,199**
5	**2000**	**Fix 500**	**2**	41,791	**551,213**
5	**2000**	**Fix 1000**	**2**	43,394	**1098,439**
5	**2000**	**Fix 1500**	**2**	42,016	**1564,008**
5	25000	Random	**2**	595,686	274,031
5	25000	Fix 100	**2**	602,815	93,091
5	25000	Fix 500	**2**	667,228	142,655
5	25000	Fix 1000	**2**	733,804	205,495
5	25000	Fix 1500	**2**	694,330	237,844
5	**55000**	**Random**	**2**	**244,038**	**277,110**
5	**55000**	**Fix 100**	**2**	**235,260**	**138,478**
5	**55000**	**Fix 500**	**2**	**246,570**	**259,718**
5	**55000**	**Fix 1000**	**2**	**268,383**	**339,202**
5	**55000**	**Fix 1500**	**2**	**249,164**	**519,349**

EAP-TLS (RADIUS SERVER) -WEP 64 BIT-UDP

Security Layer	*Outgoing Bandwidth*	*Packet Length*	*# of clients*	*UDP Throughput (Kbytes/sec)*	*UDP Response Time(sec)*
5	**2000**	**Random**	**1**	**48,446**	**198,350**
5	**2000**	**Fix 100**	**1**	**51,255**	**38,923**
5	**2000**	**Fix 500**	**1**	**51,074**	**129,632**
5	**2000**	**Fix 1000**	**1**	**52,106**	**260,673**
5	**2000**	**Fix 1500**	**1**	**51,929**	**435,233**
5	25000	Random	**1**	805,945	39,049
5	25000	Fix 100	**1**	744,494	23,718
5	25000	Fix 500	**1**	771,806	34,812
5	25000	Fix 1000	**1**	875,850	42,201
5	25000	Fix 1500	**1**	772,496	58,293
5	**55000**	**Random**	**1**	**709,014**	**51,148**
5	**55000**	**Fix 100**	**1**	**640,286**	**23,671**
5	**55000**	**Fix 500**	**1**	**650,595**	**35,764**
5	**55000**	**Fix 1000**	**1**	**723,279**	**42,183**
5	**55000**	**Fix 1500**	**1**	**685,305**	**63,175**
5	**2000**	**Random**	**2**	**47,856**	**225,626**
5	**2000**	**Fix 100**	**2**	**50,137**	**68,485**
5	**2000**	**Fix 500**	**2**	**49,930**	**122,611**
5	**2000**	**Fix 1000**	**2**	**51,548**	**271,318**
5	**2000**	**Fix 1500**	**2**	**51,371**	**476,744**
5	25000	Random	**2**	748,456	75,052
5	25000	Fix 100	**2**	714,159	41,251
5	25000	Fix 500	**2**	813,390	47,688
5	25000	Fix 1000	**2**	863,394	368,505
5	25000	Fix 1500	**2**	860,446	104,287
5	**55000**	**Random**	**2**	**636,286**	**49,165**
5	**55000**	**Fix 100**	**2**	**592,105**	**26,379**
5	**55000**	**Fix 500**	**2**	**605,141**	**32,920**
5	**55000**	**Fix 1000**	**2**	**632,370**	**41,342**
5	**55000**	**Fix 1500**	**2**	**594,396**	**68,346**

EAP-TLS (RADIUS SERVER) -WEP 128 BIT –TCP

Security Layer	*Outgoing Bandwidth*	*Packet Length*	*# of clients*	*TCP Throughput (Kbytes/sec)*	*TCP Response Time(sec)*
6	**2000**	**Random**	**1**	**37,562**	**796,135**
6	**2000**	**Fix 100**	**1**	**38,755**	**450,996**
6	**2000**	**Fix 500**	**1**	**38,783**	**574,496**
6	**2000**	**Fix 1000**	**1**	**41,270**	**1075,368**
6	**2000**	**Fix 1500**	**1**	**39,197**	**1108,244**
6	25000	Random	**1**	580,339	460,920
6	25000	Fix 100	**1**	577,397	174,223
6	25000	Fix 500	**1**	592,399	153,273
6	25000	Fix 1000	**1**	657,215	145,554
6	25000	Fix 1500	**1**	638,690	243,692
6	**55000**	**Random**	**1**	**239,985**	**211,715**
6	**55000**	**Fix 100**	**1**	**265,451**	**49,702**
6	**55000**	**Fix 500**	**1**	**272,183**	**92,625**
6	**55000**	**Fix 1000**	**1**	**305,767**	**134,527**
6	**55000**	**Fix 1500**	**1**	**254,393**	**253,667**
6	**2000**	**Random**	**2**	**36,927**	**796,140**
6	**2000**	**Fix 100**	**2**	**37,368**	**448,791**
6	**2000**	**Fix 500**	**2**	**38,500**	**587,825**
6	**2000**	**Fix 1000**	**2**	**39,976**	**1172,149**
6	**2000**	**Fix 1500**	**2**	**38,707**	**1667,252**
6	25000	Random	**2**	548,766	292,265
6	25000	Fix 100	**2**	555,334	100,349
6	25000	Fix 500	**2**	614,674	152,175
6	25000	Fix 1000	**2**	676,006	219,367
6	25000	Fix 1500	**2**	639,641	254,697
6	**55000**	**Random**	**2**	**244,037**	**295,523**
6	**55000**	**Fix 100**	**2**	**235,259**	**147,686**
6	**55000**	**Fix 500**	**2**	**246,568**	**277,878**
6	**55000**	**Fix 1000**	**2**	**268,381**	**361,679**
6	**55000**	**Fix 1500**	**2**	**249,162**	**553,555**

EAP-TLS (RADIUS SERVER) –WEP 128 BIT-UDP

Security Layer	*Outgoing Bandwidth*	*Packet Length*	*# of clients*	*UDP Throughput (Kbytes/sec)*	*UDP Response Time(sec)*
6	**2000**	**Random**	**1**	**50,999**	**196,482**
6	**2000**	**Fix 100**	**1**	**53,956**	**36,650**
6	**2000**	**Fix 500**	**1**	**53,766**	**124,632**
6	**2000**	**Fix 1000**	**1**	**54,852**	**249,404**
6	**2000**	**Fix 1500**	**1**	**54,666**	**443,397**
6	25000	Random	**1**	848,419	38,785
6	25000	Fix 100	**1**	783,730	21,611
6	25000	Fix 500	**1**	812,481	36,559
6	25000	Fix 1000	**1**	922,009	45,188
6	25000	Fix 1500	**1**	813,208	60,034
6	**55000**	**Random**	**1**	**709,013**	**51,736**
6	**55000**	**Fix 100**	**1**	**640,286**	**22,658**
6	**55000**	**Fix 500**	**1**	**650,595**	**33,596**
6	**55000**	**Fix 1000**	**1**	**723,278**	**45,097**
6	**55000**	**Fix 1500**	**1**	**685,305**	**67,031**
6	**2000**	**Random**	**2**	**50,402**	**226,589**
6	**2000**	**Fix 100**	**2**	**52,804**	**65,996**
6	**2000**	**Fix 500**	**2**	**52,586**	**124,937**
6	**2000**	**Fix 1000**	**2**	**54,289**	**268,102**
6	**2000**	**Fix 1500**	**2**	**54,103**	**472,860**
6	25000	Random	**2**	788,266	79,929
6	25000	Fix 100	**2**	752,145	44,786
6	25000	Fix 500	**2**	856,653	47,786
6	25000	Fix 1000	**2**	909,317	368,023
6	25000	Fix 1500	**2**	906,212	113,975
6	**55000**	**Random**	**2**	**636,153**	**50,066**
6	**55000**	**Fix 100**	**2**	**591,980**	**26,669**
6	**55000**	**Fix 500**	**2**	**605,014**	**33,729**
6	**55000**	**Fix 1000**	**2**	**632,237**	**42,763**
6	**55000**	**Fix 1500**	**2**	**594,272**	**69,042**

ÖZGEÇMİŞ

Gülsüm Zeynep GÜRKAŞ 17 Temmuz 1981 tarihinde Kırklereli'nin Kaynarca beldesinde doğdu. 1999 yılında birincilikle bitirdiği lise öğreniminden sonra aynı yıl İstanbul Üniversitesi Bilgisayar Mühendisliği bölümüne girmeye hak kazandı ve 2003 yılında lisans eğitimini tamamladı.
Lisans eğitimi boyunca 1,5 yıl boyunca Beko Elektronik'te yarı zamanlı olarak çalıştı.
Ekim 2003 tarihinde İstanbul Üniversitesi Bilgisayar Mühendisliği Anabilim Dalında yüksek lisans eğitimine başladı. Aralık 2003 tarihinde ise aynı bölümde araştırma görevlisi olarak göreve başlamıştır ve halen bu göreve devam etmektedir. Çalışma konuları bilgisayar ağları ve güvenliği üzerinedir.