KABLOSUZ TASARSIZ AĞLARDA KİMLİK DOĞRULAMA PROTOKOLLERİ

Rustam BABAYEV

YÜKSEK LİSANS TEZİ
BİLGİSAYAR BİLİMLERİ

GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ

MAYIS 2011
ANKARA

Rustam BABAYEV tarafından hazırlanan KABLOSUZ TASARSIZ AĞLARDA KİMLİK DOĞRULAMA PROTOKOLLERİ adlı bu tezin Yüksek Lisans tezi olarak uygun olduğunu onaylarım.

Doç. Dr. M. Ali AKCAYOL
Tez Yöneticisi

Bu çalışma, jürimiz tarafından oy birliği ile Bilgisayar Bilimleri Anabilim Dalında Yüksek lisans tezi olarak kabul edilmiştir.

Başkan : Doç. Dr. O. Ayhan ERDEM

Üye : Doç. Dr. M. Ali AKCAYOL (Danışman)

Üye : Yrd. Doç. Dr. Suat ÖZDEMİR

Üye : _____

Üye : _____

Tarih : 26/05/2011

Bu tez, Gazi Üniversitesi Bilişim Enstitüsü tez yazım kurallarına uygundur

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada orijinal olmayan her türlü kaynağa eksiksiz atıf yapıldığını bildiririm.

Rustam BABAYEV

KABLOSUZ TASARSIZ AĞLARDA KİMLİK DOĞRULAMA PROTOKOLLERİ
(Yüksek Lisans Tezi)

Rustam BABAYEV

GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ
Mayıs 2011

ÖZET

Sıradan kablolu bağlantılara göre, kablosuz ağlar kullanıcılarına birçok avantaj sunmaktadır. Fakat bunun yanısıra, kablosuz ağlar için güvenli koşulların sağlanması da oldukça gereklidir. Standart kablolu bağlantılarda, yerel ağlara müdahele etmenin daha zor olmasına rağmen, kablosuz bağlantılar bu konuda çok daha hassas kalmaktadır. Bu tez çalışmasında, günümüzde giderek daha çok yaygınlaşan kablosuz ağ teknolojileri araştırılmıştır. Ağların yapısı, özellikleri, güvenlik durumları incelenerek sunulmuştur. Ayrıca, tasarsız kablosuz ağlarda güvenlik yöntemi olarak nitelendirilen kimlik doğrulama, yetkilendirme süreçlerinin öneminden bahsedilmiş ve farklı kimlik doğrulama protokollerinin çalışma prensipleri araştırılmıştır. Çalışmanın uygulama kısmında Delphi platformu kullanılarak, ağlarda kimlik doğrulama benzetimi yapılmıştır.

Bilim Kodu : **702.1.014**
Anahtar Kelime : **kimlik doğrulama, tasarsız kablosuz ağlar, güvenlik protokolleri, şifreleme**
Sayfa Adedi : **63**
Tez Yöneticisi : **Doç. Dr. M.Ali AKCAYOL**

AUTHENTICATION PROTOCOLS ON WIRELESS AD HOC NETWORKS

(M. Sc. Thesis)

Rustam BABAYEV

GAZI UNIVERSITY

INFORMATICS INSTITUTE

May 2011

ABSTRACT

Comparatively with classical wired networks, wireless networks offer many advantages to their users. But in addition to this, it is very important to provide secure conditions for such network. In classic wired connections, it is difficult to interrupt local networks, but wireless connections have much more sensibilities about it. In this thesis, were mentioned wireless network technologies, which are getting more popular. Structure, properties, security conditions of networks analyzed and presented. Also several security techniques on ad hoc wireless networks, like authentication, authorization were mentioned and principles of several authentication protocols researched. At the implementation part of this study, there was applied authentication simulation using Delphi platform.

Science Code : **702.1.014**
Key Words : **authentication, ad hoc wireless networks, security protocols, encryption**
Page Number : **63**
Adviser : **Assoc. Prof. Dr. M.Ali AKCAYOL**

TEŞEKKÜR

Çalışmalarımın başından sonuna kadar çok değerli tavsiye ve katkılarıyla beni yönlendiren sayın hocam Doç. Dr. M. Ali AKCAYOL`a, bu aşamaya kadar gelmemde emeği geçen tüm bölüm hocalarıma, ayrıca enstitümüz öğrenci işlerine, maddi ve manevi desteklerini hiçbir zaman esirgemeyen çok değerli arkadaşlarıma ve her zaman yanımda olan sevgili anne ve babama teşekkürü borç bilirim.

İÇİNDEKİLER

Sayfa

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

Şekil **Sayfa**

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış bazı simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	**Açıklama**
ACL	Asynchronous Connection-Oriented Link
AKE	Asymmetric Key Exchange
CHAP	Challenge Handshake Authentication Protocol
EAP	Extensible Authentication Protocol
EN	Erişim Noktası
EKE	Encrypted Key Exchange
FHSS	Frequency Hopping Spread Spectrum
ICV	Integrity Check Value
IEEE	Institute of Electrical and Electronics Engineers
ISM	Industrial, Scientific and Medical
IV	Initialization Vector
MANET	Mobile Ad Hoc Networks
MIC	Message İntegrity Code
PAP	Password Authentication Protocol
PEAP	Protected Extensible Authentication Protocol
RSN	Robust Secure Network
SCO	Synchronous Connection-Oriented Link
SPAP	Shiva Password Authentication Protocol
SPEKE	Simple Password Exponential Authentication Protocol
TLS	Transport Level Security
WEP	Wired Equivalent Privacy
WPA	Wireless Protected Access

1. GİRİŞ

Teknolojinin her geçen gün gelişmesiyle birlikte, insanlara sunduğu rahatlık da artmış, bu teknolojik gelişmeler içinde bilgisayardaki gelişmeler de yerini almıştır. Bilgisayarların kullanım yaygınlığının artması, bilgisayarlarla ilgili isteklerin de artmasına neden olmuştur. İnsanların en uygun yolla ve zaman kaybına uğramadan bilgiye ulaşmak, kaynak paylaşımı, dosya paylaşımı, yazıcı paylaşımı gibi birtakım ihtiyaçlarını karşılamak istemesi, bilgisayarlar arasında bir iletişim ağı kurulmasını gerektirmiştir. Bunun üzerine yerel bilgisayar ağlarının yaygınlaşması 1980'li yıllarda başlamış ve gelişmiştir. Devamında ağ kavramı yaygınlaşmış, ihtiyaçlara göre ağ kavramları ve uygulamaları geliştirilmiştir. İlk olarak Yerel Alan Ağları (Local Area Networks – LANs) ortaya çıkmış, daha sonra daha geniş coğrafyadaki bilgisayarların birbirleriyle haberleşme ihtiyaçları Geniş Alan Ağları (Wide Area Networks - WANs) kavramının ve uygulamasının doğmasına neden olmuştur [1].

Ağların birbirleri ile haberleşmeleri, eskiden sadece kablolar sayesinde olmaktaydı. Ancak günümüzde kablosuz ağ kavramı da geliştirilmiş, avantajlarının fazla olması sonucu uygulamada yerini hızlı bir şekilde almıştır. Kablosuz ağ kablolu iletişime alternatif olarak uygulanan, radyo frekansı teknolojisini kullanarak havadan bilgi alışverişi yapan esnek bir iletişim sistemidir.

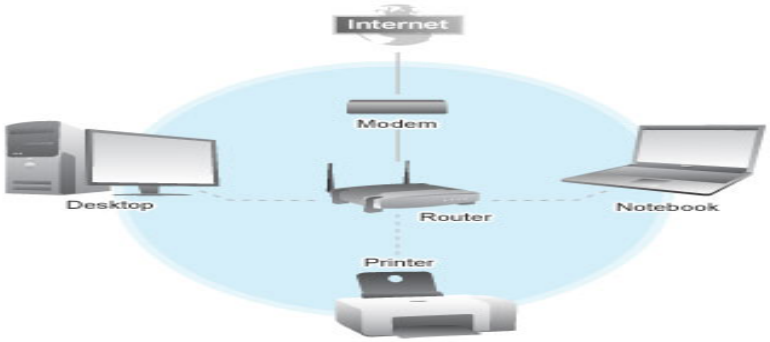
Kablosuz ağlar günümüzde sağladığı birçok fayda nedeni ile vazgeçilmezler arasındadır. Eskiden bilgisayarlar arasındaki iletişim kablolu ağlar üzerinden yapıldığından mesafe, hız, dış etkenler gibi çok sayıda engeller ortaya çıkıyordu. Şimdi kablosuz ağlar kullanıcılara büyük rahatlık ve kolay kullanım sağlamaktadır. Fakat güvenlik konusu her yerde olduğu gibi kablosuz iletişimde de göz ardı edilemez. Bilgilerin gönderilirken adrese bir bütün şeklinde, kayıpsız olarak ulaşması, gönderenin ve mesajı alan kişinin kimlik doğrulanmasına tabi tutulması, kablosuz ağlar için olmazsa olmazlardandır. Tezde kablosuz ağ teknolojileri, güvenlik yöntemleri ve protokolleri ile ilgili yoğun araştırma yapılmış, uygulama olarak da kablosuz ağlar için kimlik doğrulama sürecinin benzetimi yapılmıştır.

2. KABLOSUZ MOBİL AĞLAR

Bu bölümde kablosuz mobil ağlar, onların yapısı, özellikleri, standartları, çalışma çeşitleri, güvenlik protokolleri, avantaj ve dezavantajları incelenerek sunulmuştur.

2.1. Kablosuz Ağ Standartları

Kablosuz ağ iletişiminde standartlar *IEEE* tarafından belirlenmektedir. Kablosuz ağların standartlarını oluşturduğu grup 802.11'dir. 802.11 IEEE tarafından oluşturulmuş ilk iletişim standartıdır. 2,4 GHz ISM bandı üzerinden 2 Mbps'e kadar hız/band genişliğine sahiptir.



Şekil 2.1. Standart kablosuz ağ yapısı

802.11b - 1999 yılında ortaya çıkmıştır. Çalışma frekansı olarak 2,4 Ghz kullanmaktadır. İletişim hızı ise 11 Mbps'a kadar hız/band genişliğine sahiptir. Bu standartın kötü yanı ise bu bantta başka standartların da olması ve bu bantta çalışan diğer cihazlar ile girişim oluşma olasılığının varlığıdır.

802.11a - 2001 yılında ortaya çıkmıştır. Çalışma frekansı 5 Ghz'dir. İletişim hızı ise 54 Mbps'a kadar çıkabilmektedir.

802.11g - En son iletişim standartıdır. 802.11b'nin iletişim hızının arttırılmış versiyonu da denilebilir. Çünkü çalışma frekansı 2,4 Ghz ve iletişim hızı 54 Mbps'a kadar çıkmaktadır.

Diğer 802.11 standartları ise:

802.11f: Farklı üreticiler tarafından geliştirilmiş erişim noktalarının uyumluğunu sağlayan standarttır.

802.11i: Kablosuz ağ güvenlik esaslarını belirleyen standarttır.

802.11e: Kablosuz iletişim alanında görüntü ve ses iletimi ile ilgilenmektedir.

802.11n: 802.11 iletişim hızı arttırılması için oluşturulan standarttır [2].

2.2. Kablosuz Ağların Avantaj ve Dezavantajları

Her bağlantı türünde olduğu gibi, kablosuz iletişimin de bazı avantajları ve dezavantajları vardır.

Kablosuz ağların avantajları gibi nitelendirilebilen özellikleri bunlardır:

- *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 ölçüde özgürlük sağlamakta ve verimliliği arttırmaktadır.
- *Kolay Kurulum:* Kolay kurulumu da kendi içinde iki fayda olarak inceleyebiliriz.
  a. Zaman: Radyo dalgaları ile iletişim yapılmasından dolayı kablolu bir ağ tasarlanmasından önce gerekli olan kablolama planı ve kablolama işlemi için harcanan zamandan kazanılmış olunur.
  b. Para: 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 kablosuz yapılarda bu tip problemlerle karşılaşılmaz.

Kablosuz ağların dezavantajları gibi nitelendirilebilen özellikleri de bunlardır:

- *Güvenlik:* Yapılan iletişim dalgalar halinde yayıldığı için arayan giren bir kişinin dinlemesi ve verileri ele geçirmesi kablolu yapıya göre daha kolaydır.
- *İletişim Hızı:* İletişim hızı kablolu yapı kadar iyi değildir, çünkü onu etkileyen birçok faktör vardır. Bunlardan 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 istenen herhangi bir frekansta haberleşme yapılamaz.

2.3. Kablosuz Ağ Çalışma Çeşitleri

Kablosuz ağların iki tür çalışma çeşidi vardır. Bunlar erişim noktalı kablosuz ağlar ve tasarsız ağlardır.

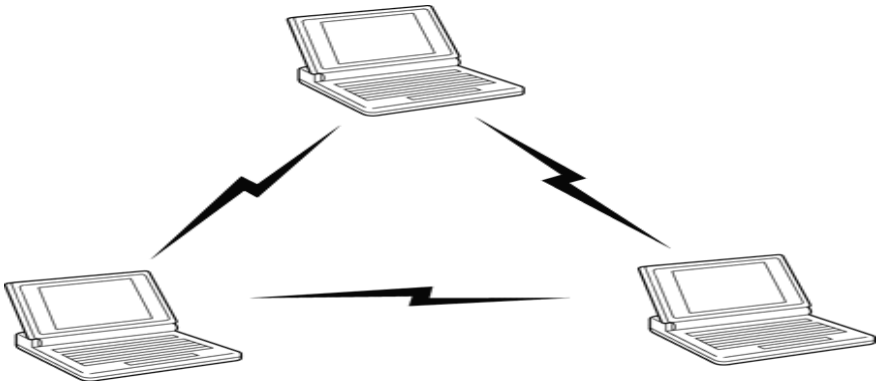
2.3.1. Erişim noktalı kablosuz ağlar

Erişim noktalı kablosuz ağların tasarsız ağlardan farkı kullanıcıların birbiri arasındaki iletişimi merkezi bir erişim noktası aracılığı ile yapmasıdır. Burada erişim noktasının görevi kablolu ağlardaki anahtarlama yapan yapılar ile aynıdır [1].

Şekil 2.2. Erişim noktalı kablosuz ağlar

2.3.2. Tasarsız ağlar

Tasarsız ağ yapısında kullanıcılar birbirileri arasında doğrudan iletişimde bulunmaktadırlar. İletişim uçtan uca (Peer to Peer - P2P) yapılmaktadır. Açık bir örnek vermek gerekirse, kablosuz LAN'ın bulunmadığı yerde iki kullanıcı kartlarını tasarsız şekilde çalışacak hale getirip birbiri ile haberleşebilir.



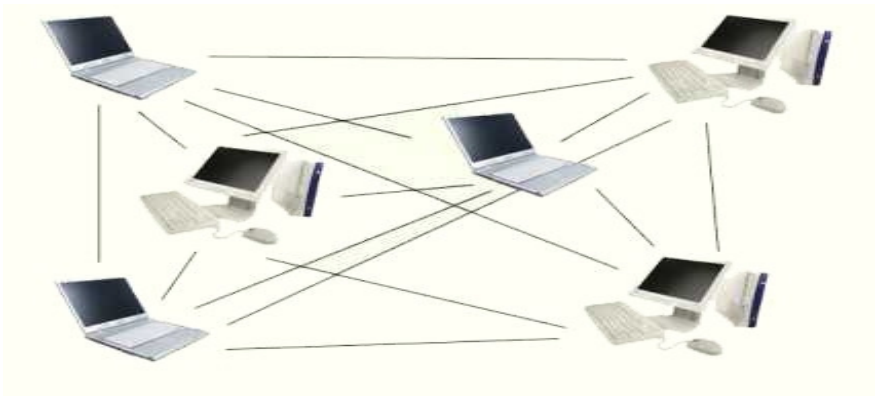
Şekil 2.3. Tasarsız ağ yapısı

Tasarsız ağlar - örneğin Bluetooth, hücresel telefonlar, dizüstü bilgisayarlar ve PDA'lar gibi aletlerin uzaktan dinamik olarak bağlanmaları için dizayn edilen ağlardır. Başka bir değişle, noktadan noktaya bağlantı anlamına gelen ad hoc bağlantı, kablosuz ağ destekli birden fazla bilgisayarın aralarında herhangi bir erişim noktası (EN) ya da hub olmaksızın birbirlerinin menzili içindeyken oluşturdukları ağa verilen ortak bir isimdir. Bu ağ sayesinde bir bilgisayar ana sunucu konumuna geçer ve diğerleri de bu bilgisayar üzerinden internete bağlanabilir. Ya da her bilgisayar, eğer aynı çalışma grubunda olacak şekilde ayarlanmışsa, birbirlerinin paylaşılan klasörlerini görebilir ve aralarında dosya alış verişi yapabilirler. Ad hoc'un gerekli olduğu durumlar şöyle sıralanabilir:

1) İnternet'e ADSL ya da Ethernet yoluyla bağlı bir bilgisayar üzerinden paylaştırmak üzere internete kablosuz olarak bağlanmak.
2) İki bilgisayar arasında dosya alışverişi yapmak.
3) Birden fazla bilgisayarın birbirlerinin dosyalarına ulaşmalarını sağlamak.

4) İnternet bağlantısının paylaşımında, yani ana bilgisayarı internete kablosuz değil de, Ethernet veya USB modem gibi bir yolla bağlamak.

Ad hoc modunda her kullanıcı, ağdaki bir diğeri ile direkt iletişim kurar. Bu mod birbirleri ile iletişim mesafesinde olan kullanıcılar için tasarlanmıştır. Eger bir kullanıcı, bu tanımlanmış mesafeden dışarıya çıkarak iletişim kurmak isterse, arada bir kullanıcı ağ geçidi ve yönlendirici olarak görev yapmak zorundadır. Ad hoc modunda peer-to-peer iletişim söz konusudur. Bu ağın bazı avantaj ve dezavantajları bulunmaktadır. En büyük avantaj kurulumun çabuk ve ucuz gerçekleştirilmesidir. Tüm yapılacak olan şey her bilgisayara bir Wi-Fi modülü takmaktır. Konfigürasyon bitirildikten sonra tüm istasyonlar birbiri ile iletişim kurabilir. İkinci avantaj ise bilgisayarların birbirlerinin üzerinden atlayabilmeleri, böylece kapsama alanının genişlemesidir. Bu sayede, eger A bilgisayarı C bilgisayarından 300 metre uzakta ise, araya bir B bilgisayarı koyarak üç bilgisayarın da birbirleri ile konuşabilmeleri sağlanır. Ancak burada sorun, eğer B bilgisayarı çökerse veya kapanırsa A ve C bilgisayarlarının birbirleri ile iletişim kuramamasıdır. Ad hoc modu maksimum bilgisayar sayısı sekiz olan ağlar için önerilmektedir. Tasarsız bağlantı zamanı iki ve daha fazla bilgisayar aynı koşullarla bir-birine bağlanabilir [3].



Şekil 2.4. Daha fazla sayıda bilgisayar için tasarsız ağ yapısı

2.4. Bluetooth Teknolojisi

Bluetooth teknolojisi son yıllarda sağlamış olduğu rahatlık ve güvenlikten dolayı çok yaygın kullanılmaya başlanmıştır. Bu teknolojinin de bazı olumlu ve olumsuz yönleri bulunmaktadır.

2.4.1. Genel bakış

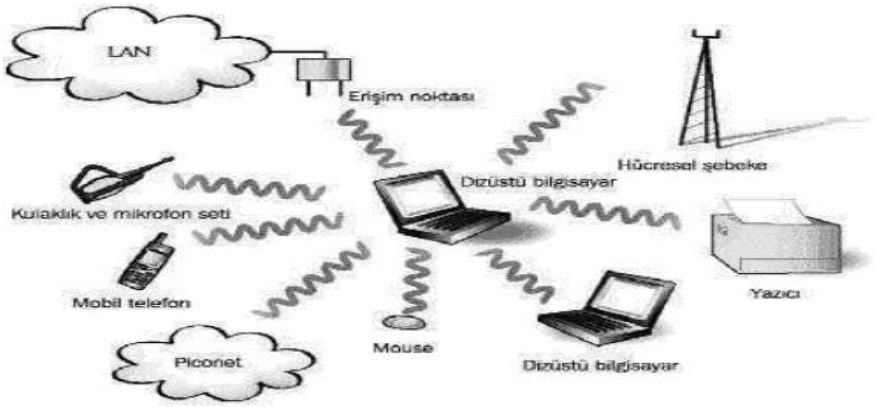
Bluetooth - Ericsson, Nokia, IBM, Intel ve Toshiba tarafından IrDA ve kablolu bağlantılara alternatif olarak geliştirilen kısa mesafede yüksek hızda veri aktarımı sağlayan güvenli bir kablosuz iletişim yöntemidir. "Yöntem" denmesinin nedeni, Bluetooth'un fiziksel araçtan, iletişim sözleşmesine kadar tamamen baştan tasarlanmış olmasıdır. Esasen beş üretici tarafından geliştirilen bu standart, halka ilk defa 1998 yılında tanıtıldı. Bluetooth kablo bağlantısını ortadan kaldıran kısa mesafe Radyo Frekansı (RF) teknolojisinin adıdır. Bluetooth bilgisayar, çevre birimleri ve diğer cihazların birbirleri ile kablo bağlantısı olmadan görüş doğrultusu dışında bile olsalar haberleşmelerine olanak sağlar. 721 Kbps`a kadar veri aktarabilen bluetooth destekli cihazların etkin olduğu mesafe yaklaşık 10 veya 100 metredir. Bluetooth 2,45 GHz ISM bandını kullanıyor. Parazitleri büyük ölçüde önleyebilmek için FHSS (Frequency Hopping Spread Spectrum) yöntemine başvuruluyor. Yöntemde 2,402 GHz ile 2,480 GHz frekans aralığı 1 MHz'lik aralıklarla 78 kanala bölünüyor. Bölünme sonucu, saniyede 1600 frekans atlaması gerçekleşebiliyor. Bu sayede de Bluetooth bağlantılar diğerlerine oranla çok daha kararlı oluyorlar [4].

2.4.2. FHSS

FHSS, tek bir taşıyıcı kullanmakta ve frekansını alıcı veya verici sinyaline göre değiştirmektedir. Frekans şemasını bilmeyen alıcılar bu sinyalleri alamaz, böylece casus dinleyicilere karşı sinyaller korunur. FHSS'te taşıma kapasitesi 2 Mbit/sn'ye kadar çıkabilmektedir. Bu ise şirket uygulamaları için uygun değildir.

Bluetooth'un Genel Özellikleri	
Frekans Aralığı	2.402 - 2.480 gHz
Veri Oranı	1 Mbps (fiziksel)
Kanal Band Genişliği	1 mHz
Menzil	~10 , ~100 metre
Frekans Atlama	1600 kez/sn
Şifreleme	48bit cihaz ID ve Eo 128bit rasgele veri şifreleme
IEEE Standartları	802.15.1 , 802.15.2 , 802.15.3 , 802.15.4
Piconet'deki aktif cihaz sayısı	1 Master 7 Slave
En fazla veri paket uzunluğu	2.745 bit

Şekil 2.5. Bluetooth teknik veriler



Şekil 2.6. Bluetooth teknolojisinin kullanımı

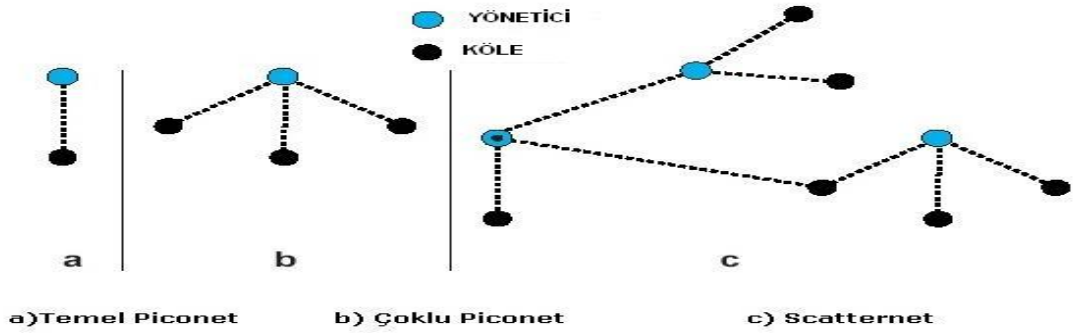
Konuşma seslerinin iletimi için Bluetooth SCO/Simetrik Bağlantı Oryantasyonu yöntemini, veri iletimi için de ACL/Asimetrik Bağlantı Yöntemini kullanıyor. Asimetrik bağlantılarda bir yöne doğru azami aktarım hızı 721 Kbit/sn, tersi yöne doğru ise 57,6 Kbit/sn olarak gerçekleşiyor. Simetrik olarak 432,6 Kbit/sn'lik veri aktarım hızıyla bağlantı kuruluyor.

Şekil 2.7. Uluslararası radyo frekans aralıkları

Bluetooth ile hem noktadan noktaya (*point to point)*, hem de noktadan birkaç noktaya (*point to multipoint)* bağlantıları kurmak mümkündür. En az iki, en çok sekiz cihazın yerel olarak birbirine bağlanması ile oluşan ağa "piconet" deniliyor. Bu ağda bütün katılımcılar teorik olarak aynı yetkilere sahiptir. Bir cihaz birden çok Piconet'e bağlı olabilir, ancak bir cihazın master konumunda olup, diğerlerini senkronize etmesi gerekir. Sınırlı menzil ve aktarım hızı değerlerinden dolayı Bluetooth sisteminin, IEEE 802.11b standartına rakip olması şimdilik düşünülemez.

2.4.3. Bluetooth'da kullanılan topoloji

Bluetooth araçları Piconet ve Scatternet adını verdiğimiz ağlar içerisinde yer alırlar ve haberleşirler.



Şekil 2.8. Bluetooth'da kullanılan topoloji

Karşılıklı olarak yarıçapı içinde olan iki araç birbirleri ile bağlantı kurabilirler. Bir bağlantı kuran araçlar bir Piconet oluşturmaktadır. Şekil 2.8'de gördüğümüz şema bir Piconet'i simgelemektedir. Bir Piconet'te bulunan araçlardan birisi yönetici rolü üstlenir. Yönetici araç içindeki bütün köleler listesini tutar. Her Piconet'te sadece bir yönetici bulunur.

Köleler ise aktif olup olmadıklarına göre sınıflandırılabilirler. Aktif bir köle, o anda yönetici ile veri aktarımı yapmakta demektir. Bir Piconet'te 255 pasif, 7 tane de aktif köle bulunabilir. Bir köle sadece yönetici ile iletişim kurabilir.

Her Bluetooth aracının kendisine ait bir Bluetooth Araç Adresi (BD_ADDR) vardır. Bu adres her araç için tektir. Yani aynı adrese sahip iki araç olamaz. Piconet'lerde aktif kölelere birer aktif üye adresi de (AM_ADDR) verilir. Bir köle aktif değilken bile yönetici ile eşzamanlı olmak zorunda olacağı için bir pasif üye adresi alır (PM_ADDR). Bir köle pasiflikten aktifliğe geçerken pasif üye adresini yitirir ve yöneticiden bir aktif üye adresi alır. Ancak bu durumda Bluetooh Piconet'inde güvenlik için sağlanan frekans atlamalı sistemin çalışabilmesi için aynı anda iki aracın aynı frekansta bulunmaması gerekmektedir. Bu da ciddi bir zamanlama sorunu getirir. Yönetici aracın saati, kölelerin referans aldığı bir nokta olur ve bu sayede frekans atlamadaki eşzamanlılık sağlanır. Kesişen alanları olan Piconet'ler grubuna Scatternet adı verilir. Örneğin bir yönetici tarafından görülen bir köle, diğer kölelerin uzağında bulunduğu için onlar tarafından görülemeyebilir. Bu durumda bu köle ile yönetici ayrı bir Piconet sayılır. Elbette, bu iki Piconet'in frekans atlama sıralamaları farklı olacaktır ki, yönetici her iki Piconet`te bulunan aktif köleler ile sorunsuz haberleşebilsin. Birden fazla Piconet`te bulunan bir Bluetooth aracı, aynı anda ancak birisinde aktif durumda olabilir. Aynı zamanda, bir Piconet`te yönetici olan bir araç, diğerinde köle de olabilir.

2.4.4. Sistemin çalışması

Bluetooth araçları dört ayrı çalışma durumundan birisindedirler: aktif, koklama, durağan ve park. Bağlantı sırasında paketler gidip gelirken bu durumlardan geçilir. Aktif durumdaki bir araç, yönetici-köle kanalını kendi zaman aralığında dinleyerek, kendi AM_ADDR'sini içeren paketleri bekler. Araç sadece kendi zaman aralığında dinleme işleminde bulunduğu için aktif mod enerji anlamında en verimli durumdur. Koklama durumundaki bir köle, kanalı yönetici tarafından kendisine bildirilen bir zaman aralığında periyodik olarak dinler. Bu, özellikle birden fazla Piconet`te yer alan köleler için enerji tasarrufu yapmaya yönelik bir uygulamadır. Yönetici köleye paketleri sadece önceden belirttiği koklama zaman aralıklarında yollar. Durağan durumdaki bir köle belli işlemleri yapamaz, ancak yönetici ile frekans eş zamanlılığını korur. Bu durumdaki bir köle hala AM_ADDR'sini korur. Yani aktif duruma geçtiği zaman eski adresi ile çalışacaktır. Park durumundaki bir köle ise park

üye adresi (PM_ADDR) ve erişim isteme adresi (AR_ADDR) olarak iki adres alır. Park durumu bir yöneticiye 7'den daha fazla köle bağlandığı zaman ortaya çıkar. Park durumundaki bir köle, aktif duruma geçmek için yöneticiye AR_ADDR'i ile başvurur. AR_ADDR'lerin her köle için farklı olmak zorunda olmadığını, ancak PM_ADDR'lerin her köle için farklı olduğunu bilmemiz yararlı olacaktır. Bu sayede bir Piconet`te yer alan köle sayısı 7'den 255'e çıkartılırken iletişimin verimliliği de korunmuş olur.

2.4.5. Güvenlik ve kimlik doğrulama

'Karşılıklı Yarış' (*Challange Response*) algoritmasını kullanan Bluetooth, daha basit bir ifade ile cihazların birbirini tanımaları için gizli bir tanımlama şifresi kullanıyor. Bluetooth ile iletilen veriler, 128-bit uzunluğunda bir anahtarlama işlemi ile gönderilebiliyor. Gönderilen verilerin de işlenebilir hale gelmesi için yine 128-bit'lik bir anahtarlama kullanılıyor. Bluetooth cihazları 48-bit'lik bir adreslemeye sahiptirler. Bu da 281 milyar cihazın birbirinden ayırt edilmesinin mümkün olacağı anlamına geliyor. Ayrıca veri iletim uzaklığının kısıtlı olması da (yaklaşık 10 metre) bir güvenlik önemli olarak görülebilir. Bu fonksiyonlar sayesinde örneğin bir cep telefonu ile bir dizüstü bilgisayar haberleşirken, üçüncü şahısların araya girmesi engellenmiş olur [4].

Bluetooth'da kimlik doğrulama ve şifreleme yordamlarında kullanılan öğeler aşağıdaki çizelgede sunulmuştur.

Çizelge 2.1. Kimlik doğrulama ve şifrelemede kullanılan öğeler

ÖĞE	BÜYÜKLÜĞÜ
BD_ADDR	48 bit
Kimlik Doğrulama için Gizli Kullanıcı Anahtarı	128 bit
Şifreleme için Gizli Kullanıcı Anahtarı, ayarlanabilir uzunlukta (8 bit katları)	8 – 128 bit
RAND	128 bit

Kimlik doğrulama için gizli anahtar (Bağ anahtarı)

Kimlik doğrulama anahtarısadece iki cihazın birbirleriyle ilk iletişime geçmesi aşamasında üretilir. Bu özelliğinden dolayı da kimlik doğrulama için kullanılan bu anahtar, bağ anahtarı olarak adlandırılmıştır.

- Anahtarın uzunluğu sabit ve 128 bitdir.
- Bir kere üretildiğinde, bunu paylaşan Bluetooth cihazları arasındaki bir çok kimlik doğrulama alt bağlantılarında değiştirilmeden kullanılabilir.
- Bağ anahtarı, yarı kalıcı bir anahtardır. Bluetooth çipinde yer alan uçucu olmayan bellekte saklanır. Yarı kalıcılığı, istenildiğinde değiştirilmesinin mümkün olmasından kaynaklanmaktadır
- Farklı uygulamalara cevap verebilmek için dört tip bağ anahtarı tanımlanmıştır.
    a) İlklendirme anahtarı (the initializationkey) KİNİT
    b) Birleşim anahtarı(the combinationkey) KAB
    c) Cihaz anahtarı(the unitkey) KA
    d) Geçici anahtar (the temporarykey) KMASTER

Şifreleme için gizli anahtar

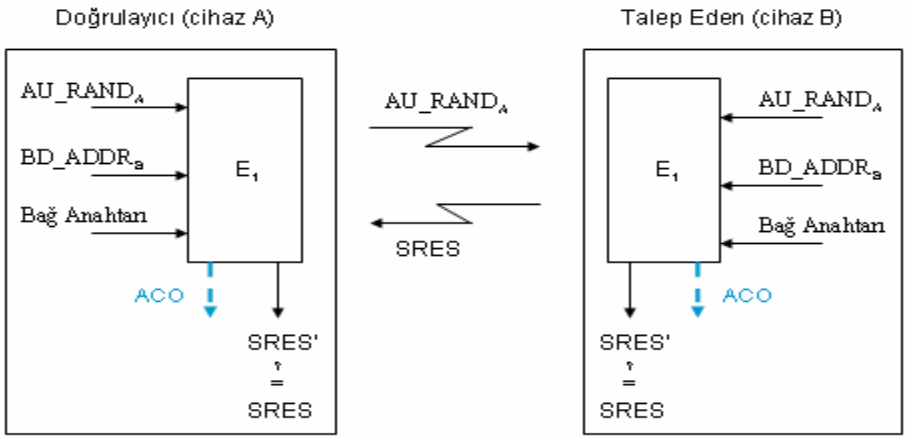
- Anahtarın uzunluğu 1 ve 16 bayt (8 –128 bit) arasında değişir.
- Uzunluğu iki nedenden dolayı değişken olarak düzenlenmiştir

    1. Birincisi, farklıülkelerde uygulamaya koyulan kriptografi algoritmaları üzerindeki ihracat düzenlemeleri;

    2. İkincisi de gelecekteki ihtiyaçlar söz konusu olduğunda, şifreleme algoritmasının hem yazılım hem de donanım olarak değiştirilmeden kolayca tekrar kullanılabilmesidir.

- Kullanılan her şifreleme algoritması için tekrar üretilir.

RAND ise cihazdaki 128 bitlik rastlantısal işlemler sonucunda elde edilen sözde rastlantısal bir sayıdır. Bu sayı iki cihazın haberleşmesi sırasında çok sık-sık değiştirilir.



Şekil 2.9. Bluetooth'da kimlik doğrulama şeması

Burada K – bağ anahtarı, E_1 – MAC kimlik doğrulama, SRES = E_1 (K, AU_RAND, BD_ADDR).

2.4.6. Bluetooth avantajları

- Veri ve ses erişim noktaları: Bluetooth kablosuz teknolojisi ile her türlü mobil veya sabit iletişim cihazı üzerinden gerçek zamanlı ses ve veri transferini kablosuz olarak gerçekleştirmek mümkün olacak.
- Kablosuz ortamlar: Bluetooth kablosuz teknolojisi ile ofislerin genel problemi olan kablo yığınları ortadan kalkacak. Günümüzde 10 metre bir menzile sahip olan bu teknoloji ilave adaptörler ile 100 metreye kadar çıkarılacak.
- Kablosuz ağ: Bluetooth teknolojisine uyumlu cihazların başka bir bluetooth teknolojisi uyumlu cihazla belli bir menzil içinde sorunsuz ve kablosuz haberleşmesi ağ yapılarını da etkileyecek. Özellikle noktadan noktaya veya çok noktalı bağlantıların desteklenmesi, yeni çözümlere fırsat verecek [5].

2.4.7. Bluetooth dezavantajları

- Bluetooth için uyumlu cihaz miktarı şu an için sadece telefon ve PC seviyesinde olduğundan dolayı, çeşitliliği az ve pille çalışan cihazlar için sürekli bağlantı kurulması durumunda pil ömrünü son derece azaltmaktadır.

• İletişim hızı düşük menzilde ve aktarım hızının şu an için yeterli seviyede olamayışı nedeniyle tam olarak bluetooth'dan verim alamıyoruz.

2.5. Güvenlik Protokolleri

Kablosuz ağların yarandığı günden onların güvenli ortamda iletişim sağlamaları için önlemlerin alınması gerekmekteydi. IEEE tarafından tasarlanan güvenlik protokolleri bu koşulları sağlamaktaydı.

2.5.1. WEP (Wired Equivalent Privacy – Kabloluya Eşdeğer Gizlilik)

Bu protokol, kablosuz ağların ilk 5 yılı için IEEE 802.11'de geçerli olan tek güvenlik protokolüdür. 2000 yılında bu protokolün zayıflıkları ortaya çıkarılmaya başlanmıştır ve birçok zayıf yönleri belirlenmiştir. Fakat herkesin kabullendiği bir gerçek var ki, WEP hiç bir güvenlik protokolü kullanmamaktan daha güvenlidir. Protokol tasarlanma aşamasında iken 802.11 standartları aşağıdaki koşulları ortaya koymaktaydı.

- Makul bir şekilde güçlü olmalı (Algoritma kolayca kırılmamalı)
- Etkili olmalı (Donanım veya yazılım ile gerçekleşebilmeli)
- İhraç edilebilir olmalı (ABD hükümeti anahtar uzunluğu kısıtlaması)
- Kullanımı isteğe bağlı olmalı

Yukarıdaki şartlar göz önüne alınarak WEP standartı oluşturulmuştur. Kullanılan şifreleme algoritması RC4, anahtar uzunluğu 40-bit veya 104-bit, IV (initialization vector) uzunluğu 24-bit olmakta, veri bütünlüğünü ICV (integrity check value) ile sağlanmaktadır. Kullanılan şifreleme algoritması RC4 (Rivest Cipher) bir akış şifreleyicisi olup simetrik anahtar kullanmaktadır [6].

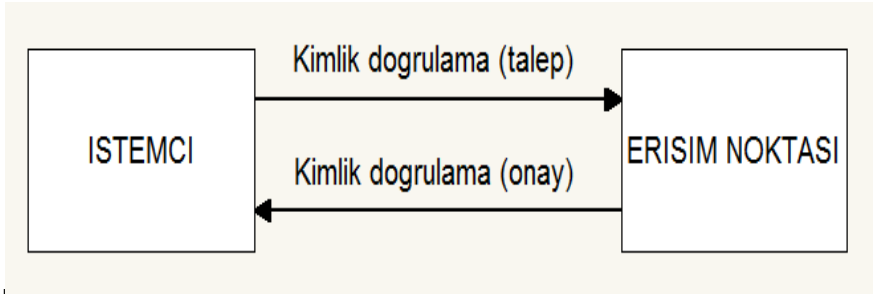
WEP'de kimlik doğrulama yöntemleri

Veri iletişimi yapılmaya başlanmadan önce kullanıcılar ve erişim noktaları arasında ilişkilendirilme yapılması gereklidir. Bu ilişkilendirilme yapılmadan önce de kimlik

doğrulama yapılması gerekmektedir. IEEE 802.11 iki farklı yöntem kullanılmakta, fakat üretici firmaların kullandığı bir yöntem çok daha sıkça uygulanmaktadır.

1) Açık güvenlik (SSID – Service Set Identifier)**:**

Bu yöntemde erişim noktasına SSID (erişim noktası ayırt edici) bilgisi ile gelen tüm kimlik doğrulama istekleri kabul edilir. Erişim noktaları SSID bilgilerini açık bir şekilde yayımlayabilirler. Ve bu gelen tüm isteklerin kabul edileceği anlamına gelmektedir.



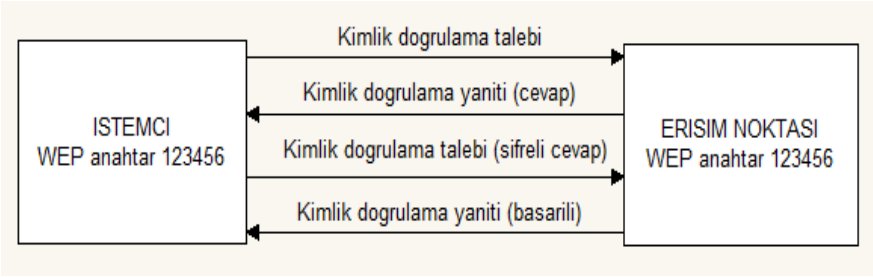
Şekil 2.10. Açık güvenlik kimlik doğrulama yöntemi

2) Ortak anahtarlı kimlik doğrulama**:**

Kimlik doğrulama paylaşılan bir anahtar sayesinde yapılır. Bu anahtar kullanıcıya daha önceden bildirilmiş olması gereklidir [7].

Çalışma yapısına bakacak olursak:

- Kullanıcı kimlik doğrulama isteği gönderir.
- Erişim noktası açık bir veri yollar.
- Kullanıcı bu veriyi ortak anahtar ile şifreleyip geri yollar.
- Erişim noktası bu şifreli veriyi açar ve gönderdiği veri ile karşılaştırıp kimlik doğrulamayı gerçekleştirir.



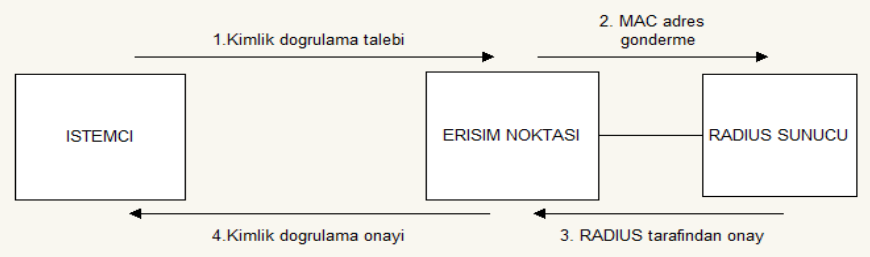
Şekil 2.11. Ortak anahtarlı kimlik doğrulama

3) MAC adresi ile kimlik doğrulama**:**

Erişim noktası üzerinden haberleşebilecek kullanıcıların MAC (Media Access Control) adresleri bir sunucuda - RADIUS'ta (Remote Authentication Dial-In User Service) tutulmaktadır. Sadece daha önceden belirlenmiş MAC adresine sahip kullanıcıların kimlik doğrulaması gerçekleştirilir.

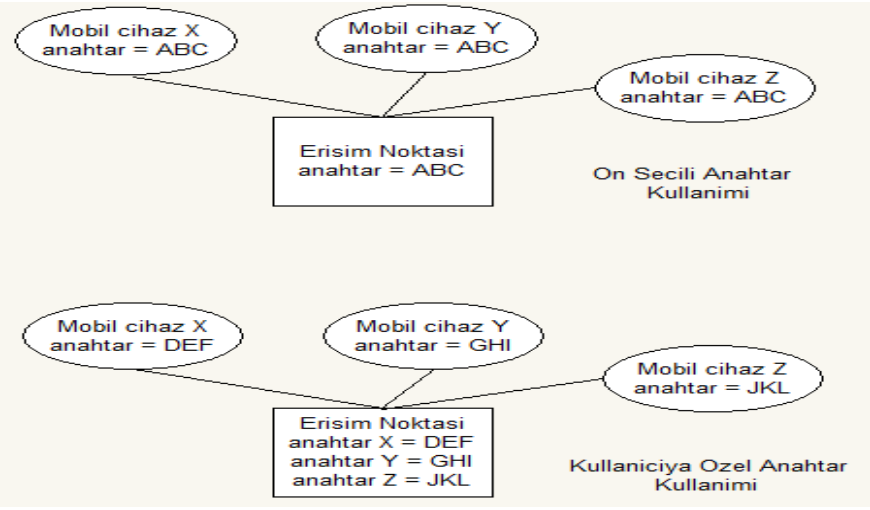
Sistemin çalışma yapısına bakacak olursak:

- Kullanıcı erişim noktasına kimlik doğrulama isteği gönderir (MAC adresi de gönderilir).
- Erişim noktası, kullanıcının MAC adresini RADIUS sunucusuna gönderir.
- Sunucu kabul ya da ret cevabını erişim noktasına gönderir.
- Erişim noktası kullanıcı için kimlik doğrulaması gerçekleştirir.



Şekil 2.12. MAC adresi ile kimlik doğrulama

WEP'de kullanılan anahtarlar



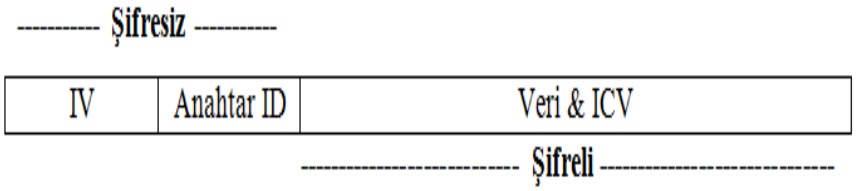
Şekil 2.13. WEP`de kullanılan anahtar çeşitleri

WEP'de kullanılabilecek anahtarlar iki gruba ayrılır. Bunlar ön seçili anahtarlar ve kullanıcıya özel anahtarlardır. Ön seçili anahtarlı yapıda erişim noktası ve kullanıcılar veri şifrelemede aynı anahtarı kullanır. Açıkça görüldüğü gibi, bu yöntem kullanıldığında tüm kullanıcılar tüm verileri çözebilirler. İkinci yöntemde ise erişim noktası her kullanıcıya karşılık farklı anahtarlar bulundurmaktadır ve bu sayede kullanıcı sadece kendine gelen verileri çözme yeteneğine sahip olacaktır.

Şifreleme ve şifre çözme

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

Şifre çözmede ise alıcı taraf IV'yi çerçeveden okur, zaten anahtar kendinde olduğu için akış şifresini elde edebilir. Şifreleme işlemlerini ters sıra ile gerçekleştirerek açık veriyi elde eder [8].



Şekil 2.14. WEP çerçeve yapısı

WEP zayıflıkları

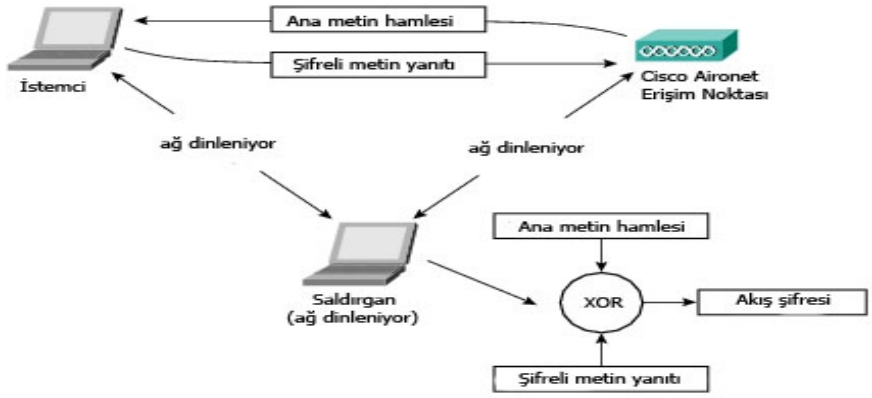
WEP güvenlik protokolü ile zayıflıklar çıktığı süreden itibaren yayımlanmaktadır. Bu protokol birçok yönden zayıf noktalara sahiptir. Aşağıda maddeler halinde bu zayıflıklar incelenmiştir.

1) Kimlik doğrulama**:**

Açık güvenlikte SSID erişim noktası tarafından yayımlanmadığı durumlarda kullanıcıların SSID'yi bilmeleri gerektiğini söylemiştik. Fakat trafiği dinleyen herhangi biri de SSID değerini alıp kullanarak kendini erişim noktasına doğrulatabilir.

MAC adresi ile kimlik doğrulamada da yukarıdaki yönteme benzer şekilde kendini doğrulayan bir kullanıcının MAC adresi trafik dinlenerek ele geçirilebilir. Ve yine bu MAC adresi kullanarak kendini doğrulatabilir.

Ortak anahtarla kimlik doğrulamada ise belirli bir IV değeri için akış şifresi ele geçirilerek kimlik doğrulama işlemi gerçekleştirilebilir. Bu işlem Şekil 2.15'te görüldüğü gibi hem açık metnin hem de şifreli halinin ele geçirilmesi ile gerçekleşir [7].



Şekil 2.15. Ortak anahtarlı kimlik doğrulamadaki zayıflık

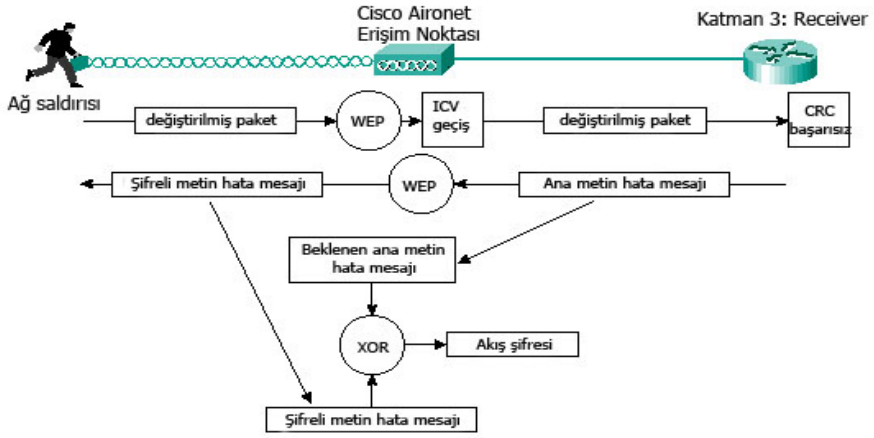
2) Tekrar saldırısı**:**

WEP`de tekrar saldırıları için herhangi bir güvenlik önlemi yoktur. Aynı mesaj defalarca gönderilebilir ve bu alıcı tarafından anlaşılamaz. Bu zayıflığı açıklamak için bir örnek verilecek olursak: Sisteme giriş yapan bir kullanıcının mesajı kimlik doğrulayıcıya giderken dinlenebilir. Kullanıcı sistemden çıktıktan sonra dinlenilen mesajlar kimlik doğrulayıcıya gönderilirse, araya giren kişi de kendini doğrulatmış olacaktır. Burada önemli bir nokta da, araya girenin mesaj içeriğini bilmesine gerek olmamasıdır.

3) Bit flapping**:**

Bu zayıflığın çıkış noktası ICV bütünlük kontrol verisinin oluşturulma şeklinden kaynaklanmaktadır. ICV lineer bir metotla oluşturulup asıl verinin sonuna eklenip şifrelenmektedir. Lineer bir metotla oluşturulduğu için şifreli olsa bile veri alanında bir değişiklik yapıldığında ICV`de oluşacak değişiklik hesaplanabilmektedir. Bu zayıflığın oluşumu Şekil 2.16`da gösterilmiş ve aşağıda maddeler halinde belirtilmiştir.

- Araya giren kablosuz ağdan bir paket alır.
- Dinlediği paketteki veri ve ICV alanlarını değiştirir.
- Bu paketi ağ dışına yollar.
- Erişim noktası ICV değerini kontrol edip çerçeveyi gönderir.
- Üçüncü katmanda CRC kontrol edilir ve belirli edilen bir hata döndürülür.
- Erişim noktası bu hatayı şifreler ve gönderir.
- Araya giren belirli hatanın hem şifreli hem de açık metnine sahip olur.
- XOR işlemi ile buradan akış şifresi elde edilir.

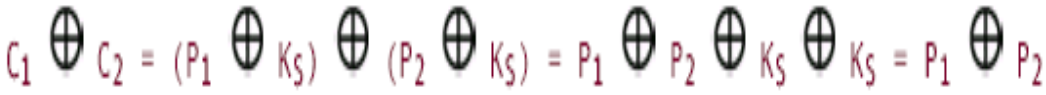


Şekil 2.16. Bit flapping

4) IV`lerin tekrar kullanılması**:**

IV`nin kullanılma amacı - aynı girişler olduğunda, çıkışların oluşturulmak istenmesidir. IV`nin 24 bit olduğunu 2^{24} yaklaşık olarak 17 milyon farklı IV anlamına geldiğini biliyoruz. Tekrarlanmadan IV birer artırarak kullanılsa bile 802.11b standartına göre yaklaşık 7 saatte tüm IV`ler kullanılmış olacaktır. Aşağıda görüldüğü gibi, XOR işlemi ve dilin yapısal özelliklerinden faydalanılarak akış

şifresi parça-parça elde edilebilir. Ve akış şifresi çözüldükten sonra bu IV ile sahte çerçeveler oluşturulabilir.



C - şifreli metin (crypted), P - açık metin (plain), K - akış şifresi (keystream)

Şekil 2.17. Initialization Vector (IV) ve akış şifresi

5) RC4 zayıf anahtarlar üretmesi**:**
RC4 algoritması bazı anahtarlardan zayıf akış şifreleri üretmektedir. Bu zayıflıktan faydalanarak şifrelenmiş metinden akış şifresini, buradan da anahtarı elde etmek mümkün olabilir.

2.5.2. WPA (Wireless Protected Access – Kablosuz Korumalı Erişim)

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

WEP`deki kusurlar 2001 yılından beri açık bir şekilde biliniyordu. IEEE 802.11`deki sorunları çözecek standartları geliştirmek için çalışmalara başladı (802.11i). Fakat bu çalışmaların ancak 2004`te bitebileceği öngörülüyordu. Endüstrinin acil ihtiyacı için 802.11i standartlarına uygun geçici bir güvenlik sistemi Wi-Fi tarafından oluşturuldu. Ayrıca hızlı bir geçiş olacağı için maliyeti düşük olmalı ve hiçbir donanım değişikliği olmamalı idi.

WPA ile WEP`in bilinen tüm zayıflıkları kapatılıyor. Donanım değişikliğine gidilmeden yükseltme (sürücü ya da firmware güncellemesi ile) yapılabiliniyor. Ayrıca, WEP'e göre bir hayli güçlü şifreleme - Temporal Key Integrity Protocol

(TKIP) ve kimlik doğrulama (802.1x) yapısına sahiptir. Bundan başka, WEP`de olmayan anahtar yönetim mekanizmasına da sahiptir. Aşağıda bu yeni özellikler açıklanmaktadır.

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

Bu algoritma RC4 akış şifreleyici algoritma üzerine kuruludur ve 4 yeni algoritma ile WEP şifreleme mekanizmasını sarar.

- IV 48 bite çıkarılmıştır ve paket numarası olarak kullanılmaktadır.
- Zayıf anahtarlar kullanılmamaktadır.
- Yeni bir mesaj bütünlük kontrol mekanizması MIC bulunuyor.
- Anahtar eldesi ve dağıtımı ile yeni bir metot getirir.
- Her çerçeve için yeni bir anahtar oluşturulur.

Bu değişiklikler sayesinde kırılamayan bir mekanizma oluşturulması hedeflenmiştir.

802.1x (EAP) ile kimlik doğrulama

802.1x EAP, IEEE`nin EAP (Extensible Authentication Protocol - Genişletilebilir Kimlik Doğrulama Protokolü) standartları üzerine kurduğu bir yapıdır. WLAN veya LAN`larda kullanılmaktadır. Şekil 2.18`da sistemin işleyişi gösterilmiştir. Yapıdaki elemanlar ise:

- Kullanıcı (Supplicant)
- Asıllayıcı ya da Erişim Noktası (Authenticator)
- Kimlik doğrulama sunucusu
- RADIUS Sunucu

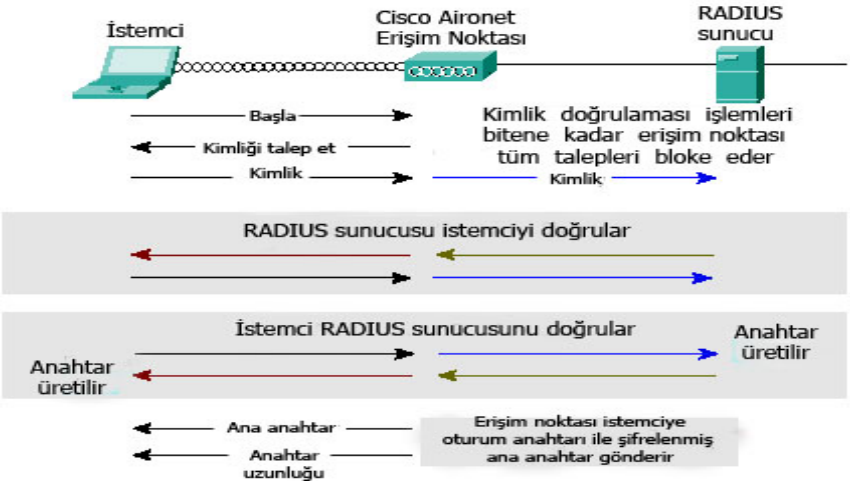
Adım-adım sistemin çalışması incelenecek olursa:

1) Kullanıcı erişim noktasına başlangıç mesajı yollar.
2) Erişim noktası kullanıcıdan kimlik bilgisi ister.
3) Kullanıcı kimlik bilgisini kimlik doğrulama sunucusuna gönderir.
4) Kimlik doğrulama sunucusu kimlik doğrulama işlemini gerçekleştirir (sayısal imza ya da başka yöntemlerle yapılabilir).
5) Kimlik doğrulama sunucusu kabul ya da ret cevabını erişim noktasına gönderir.

6) Erişim noktası bu cevabı kullanıcıya iletir ve kullanıcının ağa erişmesi için (cevap olumluysa) portlara izin verir.
7) Kullanıcı kimlik doğrulama sunucusundan kimliğini ister.
8) Kimlik doğrulama sunucusu kimliğini kullanıcıya gönderir ve kullanıcı kimlik doğrulama sunucusunu doğrular ve veri trafiği başlatır.

Görüldüğü gibi karşılıklı kimlik doğrulama yapılmaktadır. Ayrıca kimlik doğrulama sunucusu ve kullanıcı tarafından bir *ana anahtar* üretilir. Bu anahtar daha sonra geçici anahtarların üretilmesinde kullanılır. Ana anahtar erişim noktasına kimlik doğrulama sunucusu tarafından iletilir.

Eğer sistemde RADIUS yoksa, o zaman paylaşılan anahtar üzerinden kimlik doğrulama da desteklenmektedir.

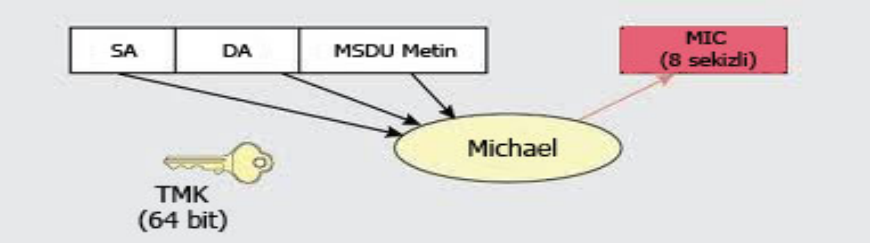


Şekil 2.18. 802.1x ile kimlik doğrulama

MIC - Message Integrity Code (Mesaj Bütünlüğü Kodu)

WEP`teki ICV`nin zayıflıkları biliniyordu. WPA ile MİChael olarak bilinen bir yöntem, 8 baytlık bir ileti bütünlüğü kodu (MIC) hesaplayan yeni bir algoritma tanımlamaktadır. MIC alanı, çerçeve verileri ve ICV ile birlikte şifrelenir. Üretilmesi ise alıcı ve gönderen MAC adresleri ile mesaj bir hash fonksiyonuna tabi tutulur ve 8 baytlık bir çıktı oluşur. MIC, IEEE 802.11 çerçevesinin veri bölümü ile 4 baytlık ICV arasına yerleştirilir ve daha sonra çerçeve verileri ve ICV ile birlikte şifrelenir. MIC lineer bir algoritma ile tasarlanmadığı için ICV gibi zayıflıkları yoktur. Bu da

araya giren kişinin mesajı değiştirdiğinde anlaşılmasını sağlar. Şekil 2.19'da MIC yapısı gösterilmektedir.

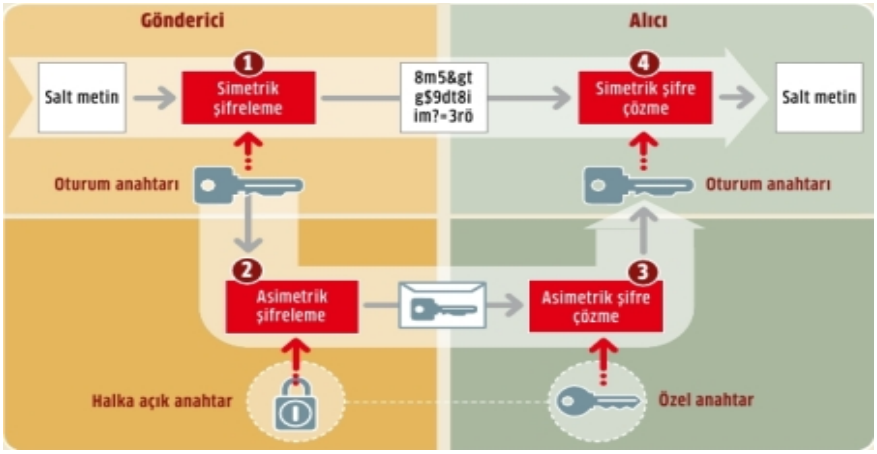


Şekil 2.19. MIC Mesaj Bütünlük Kodu

Anahtar yönetimi

WEP`den önemli bir fark olarak anahtar yönetimi gösterilebilir. WPA`da 2 çeşit anahtar yapısı vardır.

1) Oturum anahtar kümesi: İki kablosuz cihazın haberleşmesinde ve genelde bir kullanıcı ve erişim noktası arasında kullanılır (*unicast haberleşmeler*)
2) Grup anahtar kümesi: Ağ içinde herkesin bildiği ve yayım yapılması için kullanılan anahtarlar (*multicast haberleşmeler*)



Şekil 2.20. Oturum anahtarı çalışma prensibi

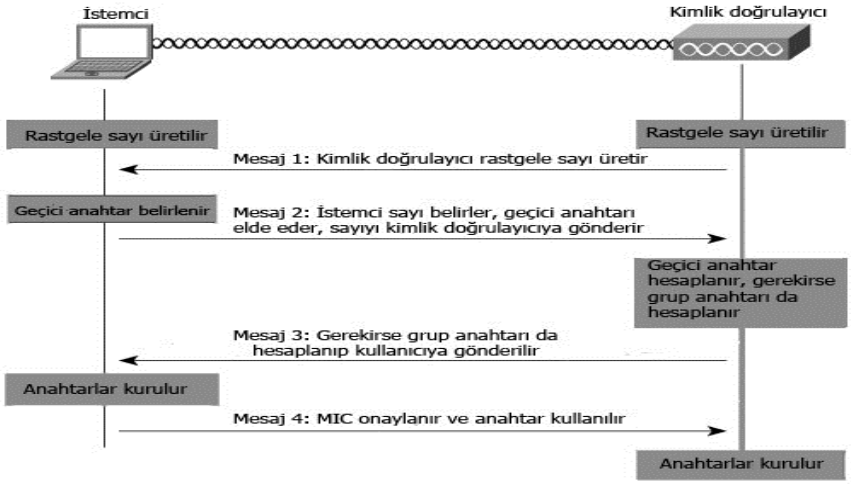
Oturum ana anahtarı ve grup ana anahtarı - ana anahtardan elde edilir. Ana anahtar da daha önceki bölümlerde belirttiğimiz gibi, kimlik doğrulama sırasında kimlik doğrulama sunucusu tarafından üretilir. Oturum ana anahtarında elde edilen anahtarlar geçicidir. Her yeni cihazla bağlantı yeniden kurulduğunda ya da ağdan çıkılıp girildiğinde yeniden oluşturulur. Üretilen anahtarların ilk ikisi - n grup anahtarları eldesinde, diğer ikisi ise şifreleme ve veri bütünlüğü için kullanılır [9].

Grup ana anahtarları da grup geçici anahtarı ile erişim noktaları tarafından belirlenip kullanıcılara dağıtılmaktadır.

Oturum anahtar kümesinin üretilmesi

Bu anahtar kümesinin eldesi erişim noktası ve kullanıcı arasında belirlenir. Belirlenme biçimi Şekil 2.21`de gösterilmiş ve aşağıda açıklanmıştır.

1) Erişim noktası rastgele sayı üretir ve kullanıcıya yollar.
2) Kullanıcı rastgele bir sayı belirler ve geçici anahtarları elde edip, rastgele sayıyı erişim noktasına yollar. MIC PMK anahtarını bildiğinin kanıtıdır. Erişim noktası geçici anahtarları hesaplar.
3) Buradan gerekirse grup anahtarlarını da hesaplayıp kullanıcıya gönderir.
4) Kullanıcı MIC`i onayladıktan sonra anahtarları kullanmaya başlar ve bunu 4. mesaj ile bildirir.
5) Erişim noktası da bu mesajı aldıktan sonra anahtarları kullanmaya başlar.



Şekil 2.21. Oturum anahtarı kümesi eldesi

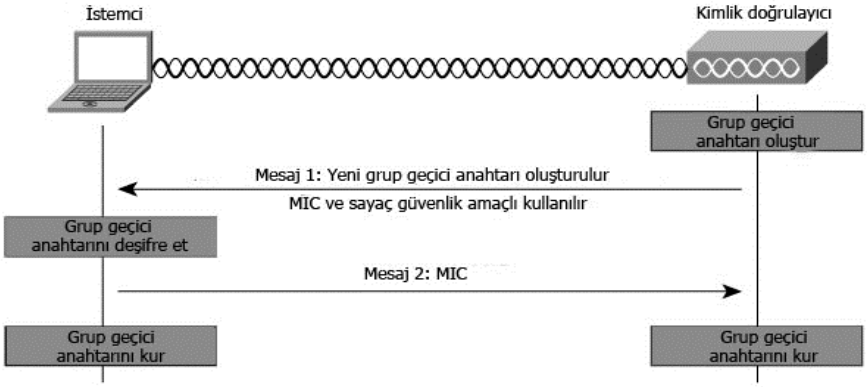
Grup anahtar kümelerinin üretilmesi

Tüm ağın haberleşileceği için farklı olan oturum anahtarları kullanılamaz. Herkesin paylaştığı bir anahtar olmalıdır ve bu da grup anahtarlarıdır. Grup anahtar kümesinin eldesi Şekil 2.22`de gösterilmiş ve aşağıda açıklanmıştır.

1) Oturum anahtarları kümesi hesaplandıktan sonra, erişim noktası grup geçici anahtarını kendi oluşturur.

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

3) Kullanıcı grup geçici anahtarını şifreyi çözerek elde eder ve kullanmaya başlar. Mesajın geçerli olduğunu belirtmek için, erişim noktasına sayacı bir artırarak MIC ile birlikte gönderir, erişim noktasında grup geçici anahtarını kullanmaya başlar.



Şekil 2.22. Grup anahtarı kümesi eldesi

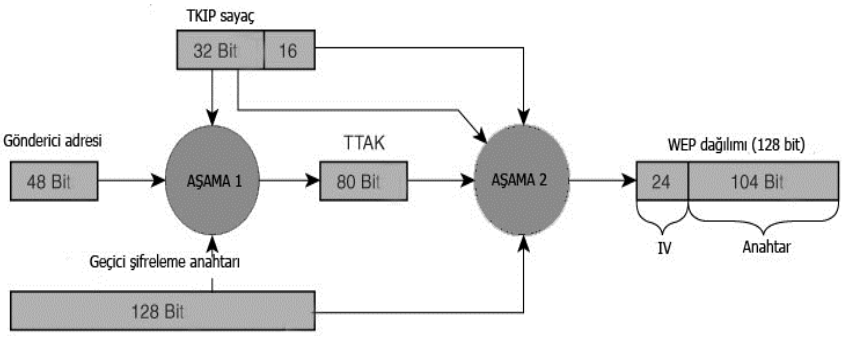
Farklı anahtar üretimi

WEP`de aynı anahtar ile şifrelenmiş çerçevelere dayalı saldırılar yapılabilmekteydi. WPA`da bu saldırıları engellemek için her paket için farklı anahtarlar üretilmesi öngörülmüştür.

Yeni anahtar hesaplamaları 2 aşamada gerçekleşir. İki aşama olmasının nedeni WEP tabanlı cihazların yüksek işlem yapabilme kapasitesinden yoksun olması ve işlem sayısını en aza indirgenmek istenmesidir.

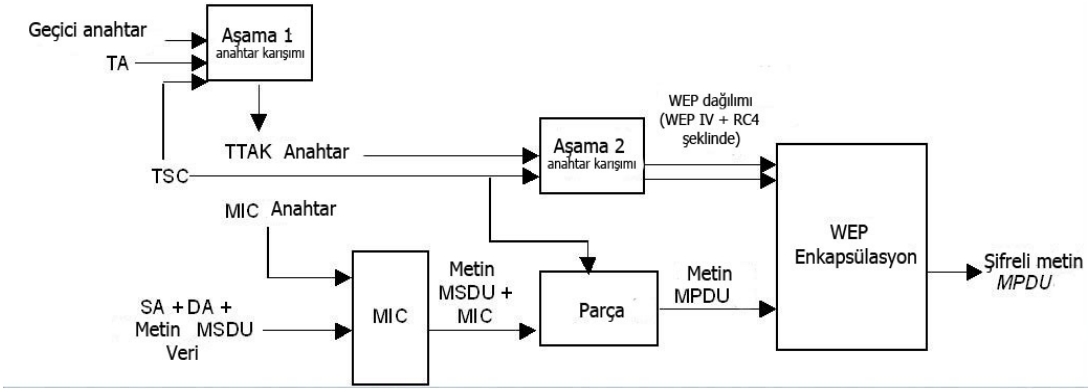
Birinci aşamada ileticinin MAC adresi, oturum ana anahtarından türetilen geçici oturum anahtarı ve IV değerinin yüksek anlamlı 32-biti XOR, AND ve S-BOX`lar gibi işlemlerden geçirilerek 80-bitlik ara anahtar elde edilir. Bu aşama 2^{16}'da bir çalışması için yeterlidir, çünkü sadece o periyotta farklı değerler üretilir. İkinci aşamada ise bu 80-bitlik ara anahtar ile IV'nin düşük anlamlı 16-biti kullanılır. Buradan 104-bitlik anahtar elde edilir. 24-bitlik IV değeri IV'nin düşük anlamlı bitlerinden türetilir.

Burada MAC adresinin kullanılma sebebi - eğer A ve B, IV değerlerini 0'dan başlatacak olurlarsa, kısa zamanda IV çatışması yaşanması engellemektir. Şekil 2.23'de farklı anahtar üretimi görülmektedir.



Şekil 2.23. Farklı anahtar üretimi

TKIP`in genel yapısına bakılacak olursa farklı anahtar üretme ile anahtar elde edilir. Mesaj bütünlük kodu hesap edilir ve mesajın sonuna eklenir. Mesaj parçalara ayrılır, parçalar IV ve anahtardan elde edilmiş akış şifresi ile şifrelenir ve alıcıya gönderilir.



DA – Destination Address (Varış adresi)

TKIP – Temporal Key Integrity Protocol (Geçici anahtar bütünlüğü protokolü)

ICV– Integrity Check Value (Bütünlük Denetim Değeri)

TSC – TKIP Sequence Counter (TKIP süreklilik sayaçı)

MPDU – Message Protocol Data Unit (Mesaj protokolü veri birimi)

TTAK– aşama 1'in sonucu (geçici anahtar ve gönderici adresi anahtar karışımı)

MSDU – MAC Service Data Unit (MAC hizmet veri birimi)

SA – Source Address (Kaynak adresi)

TA – Transmitter Address (Gönderici adresi)

Şekil 2.24. TKIP yapısı

Buraya kadar WPA'nın özelliklerini gözden geçirmiş olduk. Çizelge 2.2'de WPA'nın WEP üzerinde üstünlükleri görülmektedir.

Çizelge 2.2. WEP ve WPA karşılaştırması

	WEP	**WPA**
Şifreleme	Şifreleme yapısı kırıldı. RC4 algoritması	WEP'in açıklarını kapatıyor. TKIP/RC4 algoritması
Anahtar Uzunluğu	40 bitlik	128 bitlik
IV Uzunluğu	24 bitlik	48 bitlik
Anahtar Değişikliği	Anahtar değişimi yoktur.	Anahtarlar her oturum, her paket için değişir.
Anahtar Yönetimi	Anahtar yönetimi yoktur	802.1x
Kimlik Doğrulama	Zayıf bir yöntem	802.1x EAP ile güçlü bir yöntem
Veri Bütünlüğü	ICV	MIC

2.5.3. RSN (Robust Security Network, IEEE 802.11i, WPA2)

WPA günümüzde kırılmamış olsa da, WEP tabanlı bir yapı olduğu ve eksiklerinin çıkabileceği şüphesinden dolayı (RC4 algoritmasının zayıflıkları), IEEE 802.11i standartlarına uygun yeni bir protokol geliştirilmiştir. Bu protokol WEP üzerine kurulmamış yeni ve farklı bir yapı olarak sunulmuş, standartlaşması Mayıs 2004`te tamamlanmıştır. Ekim 2004`ten itibaren bunu destekleyen ürünler üretilmeye başlanmıştır. RSN WPA`yı desteklemekte, fakat WEP`i desteklememektedir. Çünkü WEP artık bir güvenlik unsuru olarak görülmemektedir. Piyasadaki ürünler WPA`dan RSN`e geçişi desteklememektedir, çünkü bu zaman farklı donanımsal özellikler gereklidir.

RSN kimlik doğrulamayı ve anahtar yönetimini IEEE 802.1X standartları ile gerçekleştirir. Veri bütünlüğü MIC ile sağlanır. Ayrıca gezginlik (roaming) sağlanır.

Gezginlik gerçek zamanlı iletişimlerde önem kazanır, çünkü veri kaybını engeller. RSN gezginliği iki farklı şekilde gerçekleştirir.

- Önceden kimlik doğrulama: Önceden kimlik 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 işlemlerini yapmaya kalmaz.
- Anahtar önbellekleme: Erişim noktası ile daha önceden anahtar belirlendi ise bu anahtarlar bellekte saklanır. Bu erişim noktası ile iletişime geçildiğinde 802.1x işlemlerini yapmaya kalmaz.

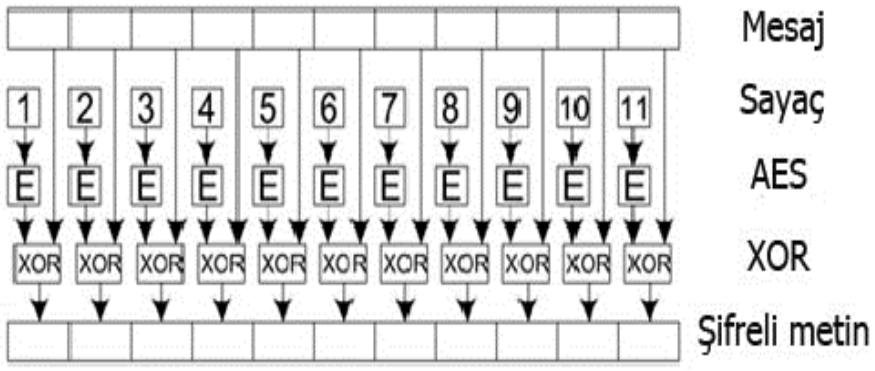
RSN'de şifreleme Temporal Key Integrity Protocol (TKIP) veya Counter Mode with CBC-MAC Protocol (CCMP) ile gerçeklenir. CCMP zorunlu iken, TKIP ise seçeneklidir.

CCMP (Counter Mode – CBC MAC protocol)

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

Counter mode (gizlilik amaçlı)

Sayaç yönteminin kullanılma amacı, aynı veri içeren bloklar aynı şifre ile şifrelendiğinde farklı çıkışların olmasının istenmesidir. Çünkü mesajın tekrar eden bloklardan oluştuğunun bilinmesi bir zayıflıktır. Şekil 2.25`de Counter mode gösterilmiştir.



Şekil 2.25. AES sayaç çalışma modu

Şekilden de görüldüğü gibi veri blokları şifrelenmiş sayılar ile XOR işlemine tutulmaktadır. Burada kullanılan sayılar rastgele seçilmektedir, çünkü aynı iki mesaj aynı çıkışları verecektir. Bu sayının başlangıcı karşı tarafa iletilmelidir. Bu modda 128-bitlik şifreleme anahtarı kullanılır.

CBC - MAC modu (bütünlük amaçlı)

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

Aşağıda MIC'in hesaplanma yöntemi verilmiştir.

1) İlk veri bloğunu al ve AES'i kullanarak şifrele;
2) Sonuç ile ikinci bloğu XOR işlemine tut ve şifrele;
3) Çıkan sonucu bir sonraki blok ile XOR işlemine tut ve şifrele;

Şifreleme yöntemi adını bu iki modun birleşiminden almaktadır.

CBC-MAC + Counter mode = CCM

CCMP çalışma yapısına bakacak olursak öncelikle MIC hesabı için CBC-MAC (Cipher block chaining message authentication code – şifreli blok zincirleme mesajı kimlik doğrulama kodu) kullanılır. Buradan oluşan 128 bitin 64 biti kullanılır.

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

Aşağıdaki çizelgede WEP, WPA ve RSN belli kriterler üzerine karşılaştırılmıştır.

Çizelge 2.3. WEP, WPA ve RSN karşılaştırması

	WEP	**WPA**	**RSN**
Şifreleme	Şifreleme yapısı kırıldı. RC4 algoritması	WEP`in açıklarını kapatıyor. TKIP/RC4	CCMP/AES CCMP/TKIP
Şifreleme Anahtarı	40 bitlik anahtar	128 bitlik anahtar	128 bit
IV Uzunluğu	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
Kimlik Doğrulama	Zayıf bir yöntem	802.1x EAP	802.1x EAP
Veri Bütünlüğü	ICV	MIC	MIC

3. TASARSIZ AĞLARDA GÜVENLİK

Tasarsız ağlar, sabit bir altyapının ve merkezi sunucuların olmadığı, kendiliğinden yapılanan ağlardır. Tasarsız ağlarda düğümler dinamik olarak, süratle ve rastgele yerleşirler. Genelde anlık bir ihtiyacı ya da belirli bir amacı yerine getirmek üzere geçici olarak oluşturulurlar. Her düğüm gerektiğinde yönlendirici olarak çalışır.

Ulusal Standartlar ve Teknoloji Enstitüsü (NIST - National Institute of Standards and Technology) tasarsız ağları iki kategoride sunmaktadır:

1) Gezgin tasarsız ağlar (Mobile Ad Hoc Networks, MANETs)
2) Duyarga ağları (Wireless Ad Hoc Sensor Networks)

Gezgin tasarsız ağlar sivil uygulamalar için daha çok tercih edilir. Daha ucuz, hafif ve kolay kullanılır olması beklenir. Dizüstü bilgisayarlar, PDA'lar gezgin tasarsız ağ uygulamalarında yaygın olarak kullanılmaktadır. Duyarga ağları ise daha çok askeri amaçlıdır. MANET'e oranla çok daha fazla düğüm içerir ve aygıtları daha kısıtlıdır. Duyarga ağları başarısız olmaya daha eğilimlidir [12].

3.1. Tasarsız Ağ Uygulamaları

Tasarsız ağlar farklı amaçlar için kullanılabilirler:

• *Askeri operasyonlarda*: Uçaklar, tanklar ve hareket halindeki kadro iletişim sağlayabilir.

• *Afet bölgesi kurtarma çalışmalarında*: Mevcut iletişim yapısının çalışmadığı sel, deprem gibi kriz yönetiminde, ilk yardım durumlarında;

• *Ticari amaçlı*: Sergilerde ya da satış sunumlarında iletişimi sağlamak için;

• *Toplantı veya konferanslarda*: Katılanların etkileşimini sağlamak için (aynı fiziksel ortamın kullanıldığı varsayımı ile, DSSS ya da FHSS);

• *Yasal zorunluluk nedeniyle***:** Sabit bir altyapının kurulmasının yasal olarak mümkün olmadığı yerlerde;

Tasarsız ağ bileşenlerinin sınırlı kaynakları yapılacak güvenlik çalışmalarını da sınırlamaktadır. Örneğin, bu kısıtlamalar küçük bir merkezi işlem birimi (CPU) ve az bellek, kısıtlı bantgenişliği ve sınırlı batarya olarak özetlenebilinir.

• *Küçük merkezi işlem birimi ve az bellek***:** İşlemcinin hesaplama gücü kısıtlı olduğundan karışık hesaplamalar yavaş yapılır.

• *Kısıtlı bant genişliği***:** Tüm iletişim telsiz ortam üzerinden gerçekleşir. Bandgenişliği kısıtlı olduğundan sabit kanal ayırma yöntemleri yerine bandgenişliğini daha etkin kullanan, hız ve erişim gecikmesi bakımından hizmet kalitesi sağlayan dinamik kanal ayırma yöntemleri uygulanmalıdır.

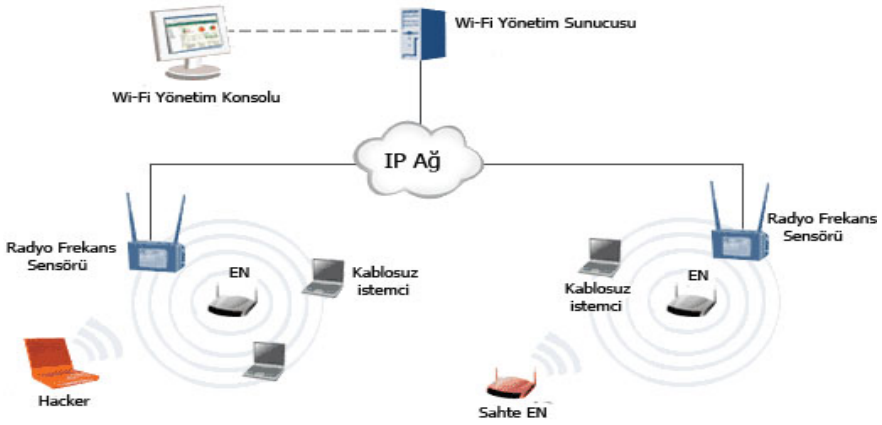
• *Sınırlı batarya***:** Batarya ömrünün sınırlı olması diğer telsiz sistemlerde olduğu gibi tasarsız ağlarda da dikkat edilmesi gereken bir unsurdur. Yol atamadaki güç tüketimi en aza indirilmeye çalışılmalıdır. Düğümler bu gücü ekonomik olarak tüketmek için alıcılarını periyodik olarak açarlar. Bu yüzden düğümlerin uyanık olduğu zamanı beklemek gerekebilir.

Tasarsız ağlarda kayda değer sıklıkta topoloji değişiklikleri beklenir. Düğümler ağa istediği zaman katılır ve istediği zaman ağı terk eder. Bunun sonucu olarak sık-sık yayınlanan güncelleme bilgileri ağ kaynaklarını meşgul eder. Bu değişiklikler ile ilgili bilginin geç gelmesi ise ağda yol atamada istikrarsızlığa sebep olur. Verimlilik (efficiency) ve yanıtlama (responsiveness) arasındaki dengeyi sağlamak oldukça zordur.

3.2. Güvenlik Sorunlarının Nedenleri ve Güvenlik Hedefleri

Tasarsız ağların altyapısının, merkezi bir denetiminin olmaması gibi karakteristik özellikleri güvenlik politikalarının gerçekleştirilmesinde kısıt olarak karşımıza çıkar.

Rastgele ve ani yerleşen kullanıcılar, dolayısıyla dinamik olarak değişen ağ topolojisi güvenlik çözümlerinin de dinamik olmasını gerektirir. Saldırıya açık telsiz ortamda çoklu iletişim ve son derece kısıtlı özkaynaklar ile daha da zorlaşan güvenlik konusu çözülmesi gereken ve hala üzerinde çalışılmakta olan bir sorundur.



Şekil 3.1. Saldırıya açık telsiz ortam

Güvenlik, özellikle güvenliğe duyarlı uygulamalarda bulunan tasarsız ağlar için önemli bir konudur. Bu konuda ulaşılması beklenen nitelikler aşağıdaki gibidir:

1. Ulaşılabilme
2. Güvenirlik
3. Bütünlük
4. Kimlik doğrulama
5. İnkar edememe

Yukarıda adı geçen özellikler tam bir mekanizmanın parçacıkları olarak nitelendiriliyor. Çünkü herhangi birinin sağlanamaması durumu büyük boyutlarda güvenlik açıklarına neden olabilir. Eğer herhangi güvenlik açıkları ortaya çıkmış olursa, böyle ağların güvenli faaliyetini sürdürebilmesi için bu açığın acil olarak kapatılması gerekmektedir [13].

3.3. Kimlik Doğrulama ve Yetkilendirme

Kimlik doğrulama ve yetkilendirme konusunun günümüzde önemini anlamak için, bir bilginin yetkisi olmayan birilerine ulaşması sonucunda nelerin olabileceğini göz önünde bulundurmak yeterli oluyordur. Belki bazı kişilerin elinde olan veriler "üçüncü" şahıslar için o kadar da önemli olmaya bilir, ancak bu verilerin banka kart şifreleri, parolalar, ulusal güvenlik bilgileri vb. şekilde olduğunu düşünecek olursak, işin boyutunun ne kadar farklara ulaştığını görüyoruz. Bu sebepten dolayı, günümüzde kimlik doğrulama ve yetkilendirme üzerine çok sayıda çalışmalar yapılmaktadır.

Kimlik doğrulama yöntemleri parmak izi veya retina deseni gibi doğrudan kullanıcıyla ilgili olan bir şeye, ya bir akıllı kart gibi sahip olunan bir şeye ya da parola veya pin gibi bilinen bir şeye dayanır. Kullanıcı adı ve şifre ile yapılan kimlik doğrulama sistemlerinde sadece kullanıcıdan gelecek şifreye göre bir doğrulama yapılması pek güvenilir olmayabilir, çünkü kullanıcı ile doğrulayıcı arasındaki ağın dinleniyor olma ihtimali ve gelen kimlik bilgilerinin başkaları tarafından değiştiriliyor olma ihtimali vardır. Bu sebeple kullanıcı ve doğrulayıcı arasında daha güvenli yöntemlerin uygulanması gerekir. Kullanıcı adı ve şifre kullanılarak yapılan kimlik doğrulama işlemlerinde düz metin şifreyi gönderip alan protokoller de mevcuttur. Şifrenin metin olarak iletişimde kullanıldığı bir protokol her türlü tehlikeye açık demektir. Kimlik doğrulama mekanizmalarını incelerken kimliklerinin doğrulanması istenen kullanıcıları istemci, doğrulayıcıları ise sunucu olarak değerlendirebiliriz. Kimlik doğrulama sistemleri iki kısımda incelenebilir. Birinci kısımda sunucu, istemcinin şifresinin düz metin halini saklar. Bir kimlik doğrulama isteği geldiğinde sakladığı bu şifre ile karşılaştırma yaparak karar verir. Bu tür mekanizmalara düz metin tabanlı mekanizmalar denir. İkinci olarak sunucunun, istemcinin şifresini direkt olarak saklamadığı, bir dizi matematiksel işlemler sonucu istemciyi doğrulayabileceği bir doğrulayıcı değer sakladığı sistemler sayılabilir. Bu sistemlere ise doğrulayıcı tabanlı sistemler denir.

Doğrulayıcı tabanlı sistemler düz metin tabanlı sistemlere göre birçok üstünlüğe sahiptir. Şifrelerin düz metin olarak saklandığı sistemlerde şifre veritabanı bir şekilde ele geçtiğinde tüm güvenlik mekanizması devre dışı kalabilir. Güvenli bir iletişim protokolünden beklenen iletişim sırasında kimlik doğrulama işleminde kullanılan değerler ile ilgili, dışarı mümkün olduğu kadar az bilginin çıkmasıdır. Doğrulayıcı tabanlı sistemlerde kullanıcı şifresi iletişimde kullanılmaz. Bu, iletişimi dinleyen bir saldırganın sisteme zarar verme ihtimalini oldukça düşürür.

3.3.1. Şifreli anahtar değişimi - Encrypted key exchange (EKE)

EKE, Diffie ve Hellman'nın (1976) genel anahtar dağıtım sistemi olarak isimlendirdikleri sisteme yapılan bir ekleme ile ortaya çıkmıştır. Bu ekleme ile, kimlik doğrulama ve iletişimde kullanılan verinin dinlenmemesi için, iletişimde gönderilen veriler gizli bir anahtar ile şifrelenmektedir. Gönderilen verinin böyle bir gizli anahtar ile şifrelenmesi iletişimi dinleyen üçüncü kişilerin kimlik doğrulama sistemi ile ilgili bilgi edinmelerini engeller.

EKE'nin gelişmiş hali olarak bir takım protokoller ortaya çıkmıştır. Bunlar arasında DH-EKE ve SPEKE sayılabilir. Bu protokollerde şifreyi ele geçiren saldırganın bu şifreyi kullanarak geçmiş veya sonraki oturumların genel anahtarlarını elde edememesi amaçlanmıştır. Buna ileri adım gizliliği (*forward secrecy*) adı verilmektedir. EKE gerçekten şifre tabanlı kimlik doğrulama protokolleri için oldukça güvenilir ve sağlam bir çözüm olmuştur. EKE'nin en büyük açık noktası, metin tabanlı şifre kullanan protokollerdeki gibi, istemci ve sunucunun aynı şifreye veya kıyım fonksiyonundan geçirilmiş haline ulaşıyor olmalarıdır. Bunun için yapılan bir çalışma yine Bellovin ve Merritt (1994) tarafından yapılmıştır. Fakat bu çalışmada eklenen özellikler *forward secrecy* özelliğini ortadan kaldırmıştır. EKE'nin bu sorununu ortadan kaldırmak için metin şifre karşılığını özel şifre dosyalarında tutan çalışmalar yapılmıştır. Bu çalışmalarda istemcinin gerçek şifresinin doğrulanması için ek bir anahtar değişimi daha getirilmiştir. Bu işlem EKE'nin bahsedilen sorununu gidermektedir. Bununla birlikte kimlik doğrulama işleminin süresini uzatmakta ve daha fazla hesaplama karmaşıklığı getirmektedir.

3.3.2. Asimetrik anahtar değişimi - Asymmetric key exchange (AKE)

EKE'de olduğu gibi AKE'nin de amacı istemci ve sunucu arasında anahtar değişimleri yapmak ve bu anahtarı kullanarak iki tarafın da belirli bir şifreyi bildiklerini doğrulamaktır. EKE'nin aksine AKE protokol akışında şifreleme kullanmaz. Bunun yerine ön tanımlı matematiksel ilişkilerden yararlanır. Şifrelemenin kullanılmamasının birçok getirisi vardır. Şifrelemenin kullanılmaması ortak bir şifreleme algoritmasının seçilmesi aşamasını kaldırdığı için, protokolde bir kolaylık sağlar. Şifreleme kullanıldığı durumda şifreleme algoritması sabitlenerek de algoritma seçim aşaması kaldırılabilir, fakat bu protokolü sadece belirli bir şifreleme algoritmasına bağımlı kılacaktır. Şifreleme kullanıldığı takdirde şifreleme algoritmasındaki herhangi bir açık doğrudan protokolün de bir açığı haline gelecektir. Ayrıca bazı şifreleme algoritmalarının kullanımı ile ilgili yasal kısıtlamalar olabilir. Bu durumda bu algoritmayı kullanan protokoller de lisans gibi konularda bağımlı hale gelecektir. Şifreleme kullanılmaması durumunda bu gibi sorunlar protokolün dışında kalacaktır.

AKE'yi diğer yöntemlerden ayıran bir özelliği daha vardır. EKE gibi protokoller kimlik doğrulama işleminin temelinde önceden tanımlanmış, paylaşılan bir şifreyi kullanırlar. Bu, sunucunun ve istemcinin aynı şifreyi sakladıkları ve kimlik doğrulama işleminde dolaylı olarak bu şifreyi kullandıkları anlamına gelir. Önceden tanımlanmış bir şifre kullanılmasına karşılık AKE bir "swaped-secret" kavramı tanımlar. Buna göre istemci ve sunucu bir şifre hesaplar. Bu şifreyi tek yönlü bir kıyım fonksiyonundan geçirerek bir doğrulayıcı üretir. Karşı tarafa bu doğrulayıcı gönderilir. Doğrulayıcıyı bir sözlük saldırısından korumak hala önemlidir, fakat çalınan bir doğrulayıcı istemciyi taklit etmek için yeterli değildir. Bunun için bu doğrulayıcıya karşılık gelen şifre de gereklidir. Bu tekniğin daha özel bir durumu olarak, sadece bir taraf bir şifre üretir ve bir doğrulayıcı hesaplar. Bu durumda başlangıçtaki şifre değişme adımları boyunca kullanıcının şifresi hiç ağa çıkmamış olur. Sadece doğrulayıcı karşı tarafa gönderilir. Bu da sistemin güvenliğini önemli derecede artırır.

3.4. Kimlik Doğrulama Protokolleri

Kimlik doğrulama protokolleri kullanıcı ile sunucu veya kullanıcıların kendi arasında güvenlik haberleşmelerini sağlamaları için gerçekleştirilen kimlik doğrulama yöntemlerini tanımlar. Aşağıda farklı kimlik doğrulama protokolleri ve kimlik doğrulama sırasında kullanılan araç ve yöntemlerle ilgili bilgiler yer almaktadır.

- Karşılıklı Kimlik Doğrulama Protokolü - *CHAP* (Challenge Handshake Authentication Protocol), kıyaslama yapıldığında, diğer kimlik doğrulama protokolü olan Parola Kimlik Doğrulama Protokolü - PAP (Password Authentication Protocol) protokolünden daha güvenli bir protokol olarak nitelendirilir.

Karşılıklı Kimlik Doğrulama Protokolü, kimlik doğrulama işlemi sırasında, kullanıcı parolanın kendisinin değil, parola gösteriminin gönderildiği, geniş çapta desteklenen bir kimlik doğrulama yöntemidir. CHAP ile uzaktan erişim sunucusu uzaktan erişim istemcisine bir kimlik sorma dizesi gönderir. Uzaktan erişim istemcisi bir karma algoritması kullanarak, kimlik sorma isteğini temel alan bir İleti Özeti-5 (MD5) karma sonucu ve kullanıcının parolasından hesaplanan bir karma sonucu hesaplar. Uzaktan erişim istemcisi MD5 karma sonucunu uzaktan erişim sunucusuna gönderir. Kullanıcının parolasının karma sonucuna da erişimi olan uzaktan erişim sunucusu, karma algoritmasını kullanarak aynı hesaplamayı yapar ve sonucunu istemci tarafından gönderilen sonuçla karşılaştırır. Sonuçlar eşleşirse, uzaktan erişim istemcisinin kimlik bilgileri gerçek kabul edilir. Karma algoritması tek yönlü şifreleme sağlar ve buna göre, bir veri bloğu için karma sonucunu hesaplamak kolaydır, ancak özgün veri bloğunu karma sonucundan hesaplamak matematiksel olarak mümkün değildir.

CHAP ters şifrelenmiş bir parola kullanımı gerektirdiğinden, MS-CHAP sürüm2 gibi farklı bir kimlik doğrulama protokolü kullanmayı düşünmemiz gerekir.

- Genişletilebilir Kimlik Doğrulama Protokolü - *EAP* (Extensible Authentication Protocol), sunucu ve istemci arasında hangi kimlik doğrulama protokolünün seçilmesi gerektiğini belirlemek için kullanılıyor.

Bu protokol rastgele uzunlukta kimlik bilgisi ve bilgi alışverişlerini kullanan rastgele kimlik doğrulama yöntemlerine izin vererek Noktadan Noktaya Protokolü'nü (PPP) genişletir. EAP, akıllı kartlar, simge kartları ve şifre hesaplayıcılar gibi güvenlik aygıtlarından yararlanılan kimlik doğrulama yöntemlerine artan talebi karşılamak üzere geliştirilmiştir. EAP, PPP içindeki diğer kimlik doğrulama yöntemlerini desteklemek için endüstri standartında bir mimari sağlar.

EAP kullanılarak, EAP türü olarak bilinen diğer kimlik doğrulama düzenleri desteklenebilinir. Bu düzenler simge kartlarını, bir defalık parolaları, akıllı kartlar ve sertifikalar kullanan ortak anahtar kimlik doğrulamasını içerir. EAP, güçlü EAP türleriyle birlikte, güvenli sanal özel ağ (Virtual Private Network - VPN) bağlantıları için çok önemli bir teknoloji bileşenidir. Sertifika tabanlı olanlar gibi güçlü EAP türleri, CHAP veya MS-CHAP gibi parola tabanlı kimlik doğrulama protokollerine göre, kaba kuvvet veya sözlük saldırıları ve parola tahminlerine karşı daha iyi güvenlik sunarlar.

EAP protokolü - rastgele bir kimlik doğrulama mekanizmasını, bir uzaktan erişim bağlantısının kimliğini doğrular. Başka EAP yöntemleri sunmak için, yönlendirme ve uzaktan erişim çalıştıran sunucuya diğer EAP modülleri takılabilir. EAP, uzaktan erişim istemcisiyle kimlik doğrulamasını yapan arasında açık uçlu bir görüşme yapılmasına olanak verir. Görüşme, kimlik doğrulamasını yapanın kimlik doğrulama bilgilerini istemesinden ve uzaktan erişim istemcisinin ona verdiği yanıtlardan oluşur. Örneğin, EAP güvenlik token kartlarıyla birlikte kullanıldığında, kimlik doğrulamasını yapan, uzaktan erişim istemcisine bir ad, PIN ve kart token değerini ayrı-ayrı sorabilir. Her sorgu sorulup yanıtlandıkça, uzaktan erişim istemcisi, kimlik doğrulamasının bir sonraki düzeyine geçer. Tüm sorular başarılı bir şekilde yanıtlandığında, uzaktan erişim istemcisi kimlik doğrulamasından geçmiş olur.

Belirli bir EAP kimlik doğrulama şeması, bir EAP türü olarak adlandırılır. Kimlik doğrulama işleminin başarıyla sonuçlandırılabilmesi için uzaktan erişim istemcisiyle kimlik doğrulayıcının aynı EAP türünü destekliyor olması gerekir.

Windows Server 2003 ailesinde, bir EAP altyapısı, iki EAP türü ve EAP iletilerini bir RADIUS sunucusuna (EAP-RADIUS) iletme yeteneği vardır.

- Parola Kimlik Doğrulama Protokolü - *PAP* (Password Authentication Protocol), eski sistemlerde kullanıldığı için, günümüzde beklenen güvenliği sağlamamaktadır.

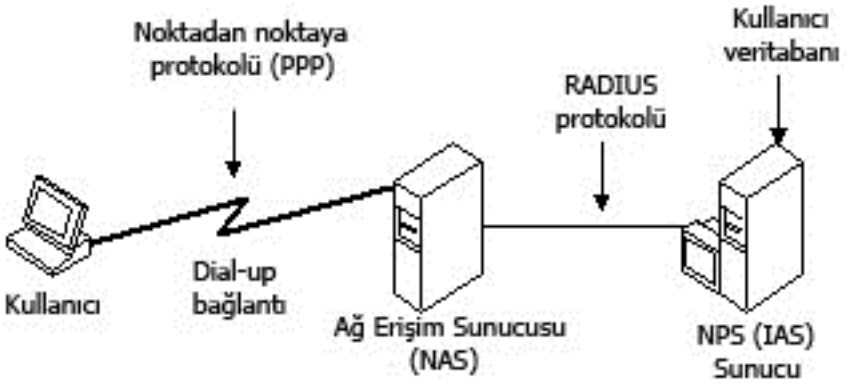
Parola Kimlik Doğrulama Protokolü düz metin parolalar kullanır ve en az güvenlik sağlayan kimlik doğrulama protokolüdür. Genellikle, uzaktan erişim istemcisi ve uzaktan erişim sunucusu daha güvenli bir doğrulama biçimini kullanarak anlaşamadığında bu protokol üzerinde anlaşılır.

Fakat PAP Windows Server 2008'e dahil edilmiştir. Bunun yapılmasının nedeni:
1) Windows 32-bit işletim sistemlerini çalıştıran uzaktan erişim istemcilerinin, güvenli bir kimlik doğrulama protokolünü desteklemeyen eski uzaktan erişim sunucularına bağlanabilmelerini sağlamak.
2) Güvenli bir uzaktan erişim protokolünü desteklemeyen Microsoft işletim sistemleri çalıştıran uzaktan erişim istemcilerinin, Windows 32-bit işletim sistemlerini çalıştıran uzaktan erişim sunucularına bağlanabilmelerini sağlamak.

- *SPAP* – Shiva PAP, Sadece NT RAS sunucularının desteklediği protokoldür.

Shiva Parola Doğrulama Protokolü (SPAP), Shiva tarafından kullanıma sunulan geri döndürülebilir bir şifreleme mekanizmasıdır. SPAP ile uzaktan erişim istemcisi, uzaktan erişim sunucusuna şifreli bir parola gönderir. SPAP çift yönlü bir şifreleme algoritması kullanır. Uzaktan erişim sunucusu parolanın şifresini çözer ve uzaktan erişim istemcisinin kimliğini doğrulamak için, düz metin biçimini kullanır. Bir Shiva istemcisinin yönlendirme ve uzaktan erişim çalıştıran bir sunucuya bağlanırken yaptığı gibi, Windows XP Professional çalıştıran bir bilgisayarda Shiva LAN Rover'a bağlanırken SPAP kullanır. Bu tür kimlik doğrulama düz metne göre daha güvenlidir, ancak CHAP veya MS-CHAP'e göre daha az güvenlidir.

- Uzaktan Kimlik Doğrulama Araması Kullanıcı Hizmeti - *RADİUS* (Remote Authentication Dial-In User Service), şirket ağında sunuculara uzaktan erişen kullanıcıların kimlik doğrulamasını sağlar.



Şekil 3.2. RADIUS ile kimlik doğrulama örneği

RADIUS endüstri standartı bir protokoldür. RADIUS - kimlik doğrulama, yetkilendirme ve hesap oluşturma hizmetleri sağlamak için kullanılır. Bir RADIUS istemcisi (genellikle bir çevirmeli sunucu, VPN sunucusu veya kablosuz erişim noktası) kullanıcı kimlik bilgilerini ve bağlantı parametresi bilgilerini bir RADIUS sunucusuna RADIUS iletisi şeklinde gönderir. RADIUS sunucusu, RADIUS istemci isteğinin kimliğini doğrular, yetkilendirir ve bir RADIUS ileti yanıtı gönderir. RADIUS istemcileri RADIUS sunucularına RADIUS hesap oluşturma iletileri de gönderir. Ayrıca, RADIUS standartları RADIUS proxy'lerinin kullanımını destekler. RADIUS proxy'si, RADIUS özelliği etkinleştirilmiş bilgisayarlar arasında RADIUS iletileri ileten bir bilgisayardır. RADIUS iletileri Kullanıcı Datagram Protokolü (UDP) iletileri olarak gönderilir. RADIUS kimlik doğrulaması iletileri için 1812 numaralı UDP bağlantı noktası, RADIUS hesap oluşturma iletileri için ise 1813 numaralı UDP bağlantı noktası kullanılır. Bazı ağ erişim sunucuları, RADIUS kimlik doğrulama iletileri için 1645 numaralı UDP bağlantı noktasını, RADIUS hesap oluşturma iletileri için ise 1646 numaralı UDP bağlantı noktasını kullanabilir. Varsayılan olarak, IAS (Internet Authentication Service) her iki UDP bağlantı noktasına ayarlanmış olan RADIUS iletilerinin alınmasını destekler. Bir RADIUS

paketinin UDP bilgilerine yalnızca tek bir RADIUS iletisi eklenir. Aşağıdaki RADIUS ileti türleri tanımlanabilir:

1) Erişim İsteği - RADIUS istemcisi tarafından bir bağlantı girişimi için istek kimlik doğrulaması ve yetkilendirme amacıyla gönderilir.
2) Erişim Onayı - Bir Erişim İsteği iletisine yanıt olarak RADIUS sunucusu tarafından gönderilir. Bu ileti RADIUS istemcisine bağlantı girişiminin kimlik doğrulamasının yapıldığını ve yetkilendirildiğini bildirir.
3) Erişim Reddi - Bir Erişim İsteği iletisine yanıt olarak RADIUS sunucusu tarafından gönderilir. Bu ileti RADIUS istemcisine bağlantı girişiminin reddedildiğini bildirir. Kimlik bilgileri özgün değilse veya bağlantı girişimi yetkilendirilmezse, RADIUS sunucusu bu iletiyi gönderir.
4) Erişim İtirazı - Bir Erişim İsteği iletisine yanıt olarak RADIUS sunucusu tarafından gönderilir. Bu ileti yanıt isteyen RADIUS istemcisine bir itirazdır.
5) Hesap Oluşturma İsteği - Kabul edilen bir bağlantının hesap oluşturma bilgilerini belirtmek için RADIUS istemcisi tarafından gönderilir.
6) Hesap Oluşturma Yanıtı - Hesap Oluşturma İsteği iletisine yanıt olarak RADIUS sunucusu tarafından gönderilir. Bu ileti, Hesap Oluşturma İsteği iletisinin başarıyla alındığını ve işlendiğini bildirir.

RADIUS iletisinde, bir RADIUS üstbilgisi ve RADIUS öznitelikleri bulunur. Bazen hiç öznitelik yoktur. Her RADIUS özniteliği bağlantı girişimi ile ilgili bir bilgi sağlar. Örneğin, kullanıcı adı, parola, kullanıcı tarafından talep edilen hizmetin türü ve erişim sunucusunun IP adresi için RADIUS öznitelikleri vardır. RADIUS öznitelikleri, RADIUS istemcileri, RADIUS proxy`leri ve RADIUS sunucuları arasında bilgi aktarmak için kullanılır. Örneğin, erişim isteği iletisindeki öznitelikler listesinde kullanıcı kimlik bilgileri ve bağlantı girişimi parametreleri ile ilgili bilgiler bulunur. Erişim onayı iletisinde ise bunun aksine, yapılabilecek bağlantı türü, bağlantı kısıtlamaları ve satıcıya özgü öznitelikler ile ilgili bilgiler bulunur.

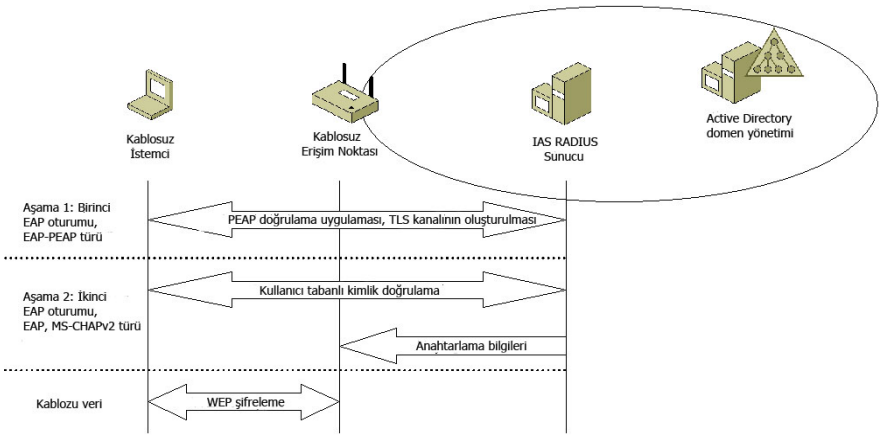
• Korumalı Genişletilebilir Kimlik Doğrulama Protokolü - *PEAP*, EAP protokollerinin bir parçasıdır. PEAP kablosuz bilgisayar gibi kimliği doğrulanan bir PEAP istemcisi ile Ağ İlkesi Sunucusu (NPS) veya başka bir RADIUS sunucusu gibi bir PEAP doğrulayıcısı arasında bir şifreli kanal oluşturmak üzere Aktarım Katmanı Güvenliği'ni (TLS) kullanır. PEAP bir kimlik doğrulama yöntemi belirtmez, ancak PEAP tarafından sağlanan TLS şifreli kanalı aracılığıyla çalışabilen Genişletilebilir Kimlik Doğrulama Protokolü - Microsoft Karşılıklı Kimlik Doğrulama Protokolü (EAP-MSCHAP v2) gibi diğer EAP kimlik doğrulama protokolleri için ek güvenlik sağlar. PEAP, aşağıdaki ağ erişim sunucusu türleri üzerinden kurulmuş ağımıza bağlanan erişim istemcileri için bir kimlik doğrulama yöntemi olarak kullanılır:

• 802.1X kablosuz erişim noktaları

• 802.1X kimlik doğrulama anahtarları

• Windows Server 2008 veya Windows Server 2008 R2 ve Yönlendirme ve Uzaktan Erişim hizmeti olarak çalışan sanal özel ağ (VPN) sunucuları

• Windows Server 2008 ve Terminal Hizmetleri Ağ Geçidi (TH Ağ Geçidi) veya Windows Server 2008 R2 ve Uzak Masaüstü Ağ Geçidi (RD Ağ Geçidi) ile çalışan bilgisayarlar.



Şekil 3.3. PEAP tabanlı kimlik doğrulama şeması

PEAP kimlik doğrulama işleminde PEAP istemcisi ile doğrulayıcı arasında iki aşama vardır. İlk aşamada, PEAP istemcisi ile kimlik doğrulama sunucusu arasında bir güvenli kanal oluşturulur. İkinci aşamada, PEAP istemcisi ile doğrulayıcı arasında EAP kimlik doğrulaması sağlanır.

Ulaşım Katmanı Güvenliği - TLS (Transport Level Security) şifreli kanalı:

PEAP kimlik doğrulamasının ilk aşamasında, PEAP istemcisi ile NPS (Network Policy Server) sunucusu arasında TLS kanalı oluşturulur. Aşağıdaki adımlarda, bu TLS kanalının kablosuz PEAP istemciler için nasıl oluşturulduğu gösterilmektedir.

1. PEAP istemcisi, NPS ile çalışan bir sunucuya RADIUS istemcisi olarak yapılandırılmış bir kablosuz erişim noktasıyla ilişkilendirilir. PEAP istemcisi ile erişim noktası arasında güvenli bir ilişki oluşturulması için, IEEE 802.11 tabanlı ilişki ilk olarak bir Açık Sistem veya Paylaşılan Anahtar Kimlik Doğrulaması sağlar.
2. İstemci ile erişim noktası arasında IEEE 802.11 tabanlı ilişki oluşturulduktan sonra, erişim noktasıyla TLS oturumu görüşülür.
3. Kablosuz PEAP istemcisi ile NPS sunucusu arasında bilgisayar düzeyinde kimlik doğrulaması başarıyla tamamlandıktan sonra, TLS oturumu bunların arasında görüşülür. Bu görüşme sırasında üretilen anahtar, kullanıcının kuruluş ağına bağlanmasına izin veren ağ erişimi kimlik doğrulaması da dahil olmak üzere sonraki tüm iletişimi şifrelemek için kullanılır [13].

EAP ile kimliği doğrulanan iletişim:

EAP görüşmesi de dahil tüm EAP iletişimi, TLS kanalı üzerinden gerçekleşir ve PEAP kimlik doğrulamasının ikinci aşamasıdır.

Aşağıdaki adımlarda önceki örnek genişletilerek, kablosuz istemcilerin PEAP kullanarak NPS sunucusuyla kimlik doğrulama işlemini nasıl tamamladığı gösterilir.

- NPS sunucusu ile PEAP istemcisi arasında TLS kanalı oluşturulduktan sonra, istemci kimlik bilgilerini (kullanıcı adını ve parolayı veya kullanıcı ya da bilgisayar sertifikasını) şifreli kanal üzerinden NPS sunucusuna aktarır.
- Erişim noktası iletileri yalnızca kablosuz istemci ile RADIUS sunucusu arasında iletir, erişim noktası (veya onu izleyen kişi) TLS uç noktası olmadığı için bu iletilerin şifresini çözemez.
- NPS sunucusu, PEAP ile kullanılmak üzere seçilen kimlik doğrulama türüyle kullanıcının ve istemci bilgisayarın kimliğini doğrular. Kimlik doğrulama türü EAP-TLS (akıllı kart veya başka bir sertifika) ya da EAP-MS-CHAP v2 (güvenli parola) olabilir.

- *TACACS* – Authentication, accounting ve authorization (AAA) sunan kimlik doğrulama protokolüdür.

TACACS+, BBN (Bolt, Beranec&Newmen, şimdi GTE Internetworking`in bir parçası) ve DOD (US Department of Defence) tarafından geliştirilmiş bir dial-up AAA metodudur. TACACS merkezi veri tabanı veya Ağ İşletim Sistemini (Network Operating System - NOS) netware gibi kullanarak kullanıcı bağlantı listelerinin bakımını sağlama fikrinden ortaya çıkmıştır. TACACS üçüncü parti kişilik belirleme sunucu sistemidir ve kullanıcı ID ve parolasını kullanarak ağa girdiğinde güvenlik sisteminin desteği ile kişilik belirlemesi yapar. Güvenlik sistemi bu kullanıcı bilgilerini kişilik belirleme için TACACS sunucuya gönderir. Bu durum aynı RAS aygıtlarının RADIUS sunucuya bağlanışı gibidir.

TACACS kullanarak, ağ içindeki çeşitli ağ bağlantı sunucuları, tek bir merkezi veri tabanı kullanarak ve böylece kişisel NAS aygıtlarındaki bilgilerin bakımını sağlayarak ve ikilemelerini elimine ederek kullanıcıların tanımlanmasını sağlarlar. CISCO firması TACACS, bunun geliştirilmiş şekli olan XTACACS ve yeni sunumu olan TACACS+`ın en güçlü destekçisi olmuştur. CİSCO 1989'dan beri TACACS ve 1990'dan beri de XTACACS`ı desteklemektedir. Ancak CİSCO artık TACACS ve XTACACS için bakım desteği sağlamamaktadır ve firma bütün gücünü yeni sürüm TACACS+ ve RADIUS üzerine yoğunlaştırmış bulunmaktadır. TACACS, CISCO System'in kurum bağımlı bir protokolüdür. TACACS'ın üçüncü sürümü olan TACACS+, fonksiyonel olarak RADIUS'a çok benzemektedir. İlk iki sürümünde TACACS kullanıcı ID/parolalar kombinasyonunu plaintext yapıda gönderirken, TACACS+ bütün bilgileri şifrelemektedir. TACACS+ bugün için yaygın olarak CISCO müşterilerince ve bir takım üniversiteler tarafından kullanılmakta ve desteklenmektedir.

- *MS-CHAP (MD4)* – Sadece Microsoft sistemlerinde çalışıyor ve veri şifrelemesi sunuyor.

Windows Server 2003 ailesi, karşılıklı kimlik doğrulama, Microsoft Noktadan Noktaya Şifreleme (MPPE) için daha güçlü başlangıç verisi şifreleme anahtarları üretimi ve gönderilen/alınan veriler için farklı şifreleme anahtarları sağlayan MS-

CHAP v2'yi destekler. Parola değiştirme sırasında parola güvenliğini tehlikeye atma riskini en aza indirmek için, daha eski MS-CHAP parola değiştirme yöntemleri desteklenmez.

MS-CHAP v2 iletişim kuralı MS-CHAP'ye göre daha güvenli olduğundan, tüm bağlantılarda (eğer etkinleştirilmişse) MS-CHAP'den önce sunulur. MS-CHAP v2 - Windows XP, Windows 2000, Windows 98, Windows Millennium Edition ve Windows sürüm NT 4.0 çalıştıran bilgisayarlar tarafından desteklenir. Windows 95 çalıştıran bilgisayarlar MS-CHAP v2'yi yalnızca VPN bağlantıları için destekler, çevirmeli bağlantılar için desteklemez.

MS-CHAP ile uzaktaki Windows tabanlı client bilgisayarlar yetkilendirilir. MS-CHAP, Message Digest 4 (MD4) hashing algoritmasını ve Data Encryption Standard (DES) şifreleme tekniğini kullanır.

3.5. Delphi'de Benzetim Uygulaması

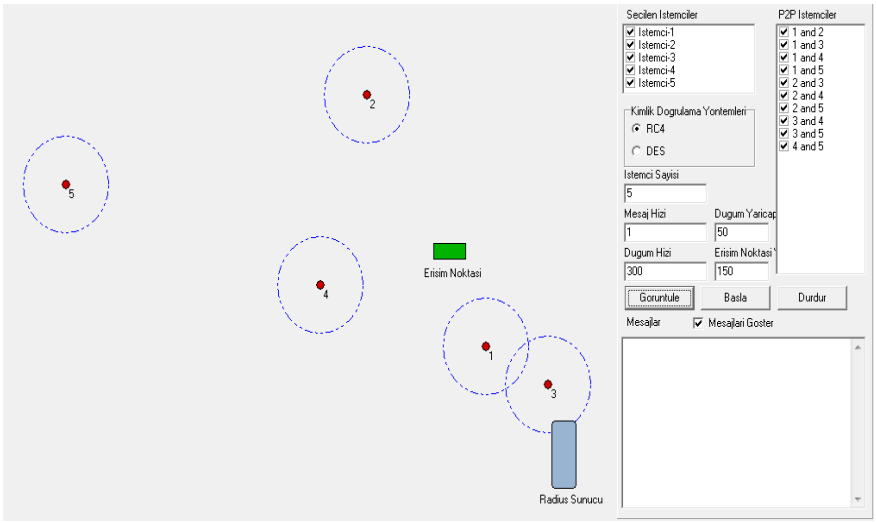
Delphi ortamında gerekli yazılım simülatörlerinin hazırlanması için birçok faydalı araç bulunmaktadır. Grafik arayüz olarak standart gri renkli arka plan ve üzerinde Edit, Memo, Button, Checkbox, Radiogroup vb. bileşenler kullanılmıştır [16].

Şekil 3.4. Benzetimin arayüzü

Benzetimde Erişim Noktası, RADIUS sunucusu ve kullanıcının belirlediği sayıda istemci arasında karşılıklı kimlik doğrulama işlemleri gerçekleştirilir.

Kimlik doğrulama protokollerinden Genişletilebilir Kimlik Doğrulama Protokolü (EAP) çalışma prenibi temel alınmış ve RC4, DES şifreleme metodları uygulanmıştır.

Simülatörü çalıştırmaya başlamazdan önce, düğümlerin, erişim noktasının kapsama alanlarının yarıçapı, istemci sayısı, düğümlerin hareket hızı, mesajların yazım hızı, mesajların görüntülenmesi, kimlik doğrulama metodunun seçimi gibi opsiyonlar sunuluyor. Şekil 3.5`de `Görüntüle` tıklandığında istemcilerin rastgele dağılımı görülmektedir. Bu zaman istemci sayısı susmaya göre, 5 olarak belirlenmiştir, bu sayı kullanıcı tarafından değiştirilebilinir.

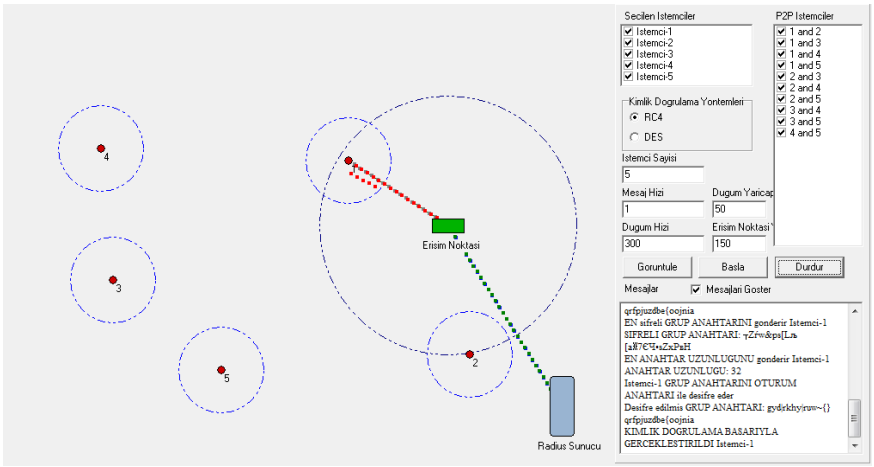


Şekil 3.5. Benzetimde istemcilerin rastgele dağılımı

`*Başla*` ve `*Durdur*` düğmeleri ile simülatör çalıştırılır ve durdurulabilir. Simülatörün çalışması zamanı düğümler rastgele yönlerde Erişim Noktası etrafında hareket ediyor. Erişim noktasının kapsama alanına girdikleri anda EAP yöntemi ile kimliklerinin doğrulanması süreci başlar. Bu zaman düğüm doğrulama talebi gönderir, erişim noktası kullanıcıyı doğrulamak için RADİUS sunucusunu kullanır. Adım-adım yeni kullanıcının kimlik doğrulaması gerçekleştirilir. Sözü geçen tüm işlemler Mesajlar bölümünde görüntülenir. Ayrıca, düğümlerin kendi aralarında da

kimlik doğrulamaları gerçekleştirilir. Program çalıştırıldığında, gerekli değişiklikler yapılabilir ve bu zaman programı çalıştıran kişinin talebine uygun şekilde işlemler uygulanır. Kimlik doğrulama – RC4 ve DES şifreleme algoritmaları vasıtasıyla gerçekleştirilir.

Benzetimde düğümlerin sabit konumda değil de, rastgele hareketli olarak sunulması – günlük yaşamda karşılaşılan gerçek ortamın en iyi şekilde bilgisayar ortamına aktarılmasını öngörmüştür. Çünkü günümüzde dinamik, yani sürekli hareket içinde olan bilgisayarlar arasında güvenli bağlantının sağlanması söz konusu olunca, gerçeklerin en doğru olacak şekilde simülasyonu, yani benzetimi en başlıca hedef olarak belirlenmiştir. Benzetimin kaynak kodu ekte sunulmuştur.



Şekil 3.6. Erişim noktası ve RADİUS sunucu kullanılarak kimlik doğrulama

4. SONUÇ

Günümüzde kablosuz ağlar gezginlik, kolay kurulum, sağlamlık gibi özellikleri ile fayda sağlamaktadır, fakat güvenlik konusu bu iletişim türünde büyük önem arz etmektedir. Tasarsız ağlar hem sivil, hem de askeri amaçlar için kullanılmaktadır. Bu sebepten en önemli mesele – gerekli güvenliğin sağlanmasıdır. Yakın tarihe göz atılırsa, ilk olarak güvenlik protokolü olarak ortaya atılan WEP, artık bir güvenlik önlemi olarak kabul görmediği izlenebilir. WEP üzerine inşa edilen ve açıklarını kapatan WPA ise, kırılmamış bir yapıya sahip olsa da RC4`ün zayıflıklarını taşımaktadır. Son olarak 2004 yılında tamamlanan RSN ise AES şifreleme algoritmasının gücü ile şu anki en sağlam güvenlik önlemlidir. Fakat RSN ile cihazlar üzerinde ciddi donanım ve yazılım değişiklikleri yapılması gerekir. Tüm bunlardan başka, kullanıcıların kablosuz ortamda bilgi paylaşımını sağlamak için tasarsız ağ yapısı giderek daha da yaygınlaşmaktadır. Ama her türlü kablosuz ağlar için güvenli bir ortamın sağlanması meselesi çok büyük önem taşımaktadır. Kablosuz ağlarda kimlik doğrulama, yetkilendirme gibi güvenlik işlemleri, bu işlemleri sağlayacak ilgili protokollerin geliştirilmesi konusu her zaman dikkat edilmesi gereken işlerdir. Bu tez çalışmasında kablosuz ağlar, onların yapıları, çalışma şekilleri, güvenlik metotları, kullanıcıların kimlik doğrulama süreçleri, protokoller ve diğer konular araştırılmış, uygulama bölümündeyse, kablosuz ağlarda kimlik doğrulama işlemi ile ilgili benzetim geliştirilmiştir. Sözü geçen benzetim Delphi araçları ile geliştirilmiş, EAP protokolünün çalışma prensibi uygulanmış, kaynak kodu ekte sunulmuştur.

Kablosuz ağlarda kimlik doğrulama sürecinin nasıl gerçekleştirildiği, benzetim uygulaması üzerinde açıkca görülmektedir. Sadece kullanıcı tarafından belirlenen istemcilerin kimlik doğrulamayı yapması, istenmeyen istemcilerin kimlik doğrulama işleminde başarısız olması, düğüm sayısının arttırılarak, daha geniş çaplı ağ yapısının benzetimi, iki farklı şifreleme yönteminin uygulanması vb. özellikler, gerçek benzetim modelini oluşturmaktadır. Yapılan derleme ve birikilen bilgilerin, ilgili konularda gelecekte yapılacak çalışmalar açısından da fayda sağlayacağına inanıyoruz.

KAYNAKLAR

1. V.Olifer, N.Olifer, "Kompyuternie Seti: Principy, Tekhnologii, Protokoly", ***4-e izdanie***, 2010.

2. Subir Kumar Sarkar, T.G.Basavaraju, C.Puttamadappa, "Ad Hoc Mobile Wireless Networks – Principles, Protocols and Applications", ***Auerbach Publications (Taylor & Francis Group LLC)***, 2008.

3. Erdal Cayırcı, Chumming Rong, "Security in Wireless Ad Hoc and Sensor Networks", ***John Wiley & Sons Ltd. Publication***, 2009.

4. Julia Layton, Marshall Brain, and Jeff Tyson, "Introduction to How Cell Phones Work", 2005.

5. Prasant Mohapatra, Srikanth V.Krishnamurthy "Ad Hoc Networks – Technologies and Protocols", ***Springer Science + Business Media Inc.***, 2005.

6. Sankar K., Sundaralingam S., Balinsky A., Miller D., "Cisco Wireless LAN Security", ***Cisco Press***, 2004.

7. K. Nichols R., C. Lekkas P., "Wireless Security Models, Threats and Solutions", 2002.

8. Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", ***Communications of the ACM***, 1978.

9. William Stallings, "Cryptography and Network Security: Principles and Practices", 4th edition, ***Prentice Hall***, 2006.

10. P. Papadimitratos, Z. Haas, "Secure Routing for Mobile Ad Hoc Networks", ***Proceedings of CNDS***, 2002.

11. Asad Amir Pirzada, Chris McDonald, "Establishing trust in pure ad-hoc networks", ***Proceedings of the 27th conference on Australasian computer science - Volume 26***, January 2004.

12. Refik Molva, Pietro Michiardi, "Security in Ad Hoc Networks", ***Proceedings PWC 2003***, September 2003.

13. Lidong Zhou, Zygmunt J. Haas, "Securing ad hoc networks", ***IEEE Networks Special Issue on Network Security***, November/December 1999.

14. Vishnevsky V.M., Lyakhov A.I., Portnoi S.L., Shakhnovich I.V., "Shirokopolosnye Besprovodnye Seti Peredachi Informacii", 2005.

15. W.Diffie and M.E.Hellman, “New Directions in Cryptography”, ***IEEE Transactions on Information Theory***, 1976.

16. Arkhangelsky A.Y., “Programmirovanie v Delphi Dlya Windows”, ***Binom Press***, 2007.

17. Aleksandr Vatataniuk, “Besprovodnaya Set Svoimi Rukami”, 2006.

18. Kuzin A.V., “Kompyuternie Seti: Uchebnoe Posobie”, ***İzdatelstvo FORUM***, 2010.

19. Anatoly Khomnenko, Vladimir Gofman, Evgeny Mescheryakov, Vladimir Nikiforov, “Delphi 7. Naibolee Polnoe Rukovodstvo”, ***BHV-Peterburg***, 2008.

EKLER

Ek-1. Delphi kodları

```
unit Unit1;

interface

uses
  Windows, Messages, SysUtils, Variants, Classes,
Graphics, Controls, Forms,
  Dialogs, ExtCtrls, StdCtrls, Math, CheckLst, RC4, DES;

type
  TForm1 = class(TForm)
    Panel1: TPanel;
    RadiusServer: TShape;
    AccessPoint: TShape;
    LabeledEdit1: TLabeledEdit;
    Memo1: TMemo;
    Label1: TLabel;
    Label2: TLabel;
    Button1: TButton;
    Label3: TLabel;
    CheckListBox1: TCheckListBox;
    Label4: TLabel;
    Image1: TImage;
    Button2: TButton;
    RadioGroup1: TRadioGroup;
    LabeledEdit3: TLabeledEdit;
    Timer1: TTimer;
    LabeledEdit4: TLabeledEdit;
    LabeledEdit5: TLabeledEdit;
    CheckBox1: TCheckBox;
    LabeledEdit2: TLabeledEdit;
    Button3: TButton;
    CheckListBox2: TCheckListBox;
    Label5: TLabel;
    procedure Button1Click(Sender: TObject);
    procedure DrawMessage(xfrom, yfrom, xto, yto: double;
color: TColor; msg: String; showmsg: boolean);
    procedure Button2Click(Sender: TObject);
    procedure DrawCircle(x, y, r: integer; color: TColor;
image: TImage; clientindex: integer);
    procedure AuthenticateWithAP(clientindex: integer;
showmsg: boolean);
    procedure Timer1Timer(Sender: TObject);
    procedure Button3Click(Sender: TObject);
  private
    { Private declarations }
```

Ek-1 (Devamı). Delphi kodları

```
  public
    { Public declarations }
  end;

const
  cnt = 50;

type
  rec = record
    dx, dy: integer;
  end;

var
  Form1: TForm1;
  count, h, speed, radius, radius2: integer;
  x1, y1, x2, y2, x3, y3: double;
  clients: array [1 .. cnt] of TShape;
  route: array [1 .. cnt] of rec;
  auth: array [1 .. cnt] of boolean;
  Data: TBitString;
  s, s1: string;
  BroadcastKey, EncyrptedKey, SessionKey: string;
  Keylength: integer;
  RC4: TRC4Context;

implementation

{$R *.dfm}

procedure TForm1.DrawMessage(xfrom, yfrom, xto, yto:
double; color: TColor; msg: String; showmsg: boolean);
var
  dx, dy: double;
  eps: double;
begin
  eps := 5;
  h := 8;
  if (xfrom <> xto) then
  begin
    dx := sign((xto - xfrom)) * h * abs
      (cos(arctan((yto - yfrom) / (xto - xfrom))));
    dy := sign((yto - yfrom)) * h * abs
      (sin(arctan((yto - yfrom) / (xto - xfrom))));
  end
  else
```

Ek-1 (Devamı). Delphi kodları

```
  begin
    dx := 0;
    dy := 0;
  end;

  while abs((xfrom + dx) - xto) > eps do
  begin
    with Image1 do
    begin
      Canvas.Brush.color := clBtnFace;
      Canvas.Brush.color := color;
      Canvas.pen.color := color;
      xfrom := xfrom + dx;
      yfrom := yfrom + dy;
      Canvas.Rectangle(round(yfrom) - 2, round(xfrom) -
2, round(yfrom) + 2, round(xfrom) + 2);
      sleep(speed);
      Application.ProcessMessages;
    end;

  end;
  if showmsg then
    Memo1.lines.add(msg);

end;

procedure TForm1.Button1Click(Sender: TObject);
begin
  Memo1.Clear;
  Timer1.Interval := StrToInt(LabeledEdit3.Text);
  Timer1.Enabled := true;
end;

procedure TForm1.Button2Click(Sender: TObject);
var
  i,j: integer;
  x, y: integer;
begin
  Randomize;
  count := StrToInt(LabeledEdit1.Text);
  radius := StrToInt(LabeledEdit4.Text);
  radius2 := StrToInt(LabeledEdit5.Text);
  for i := 1 to count do
  auth[i] := false;
  speed := StrToInt(LabeledEdit2.Text);
  radius := StrToInt(LabeledEdit4.Text);
```

Ek-1 (Devamı). Delphi kodları

```
  Image1.Canvas.Brush.color := clBtnFace;
  Image1.Canvas.FillRect(Canvas.ClipRect);
  Image1.Canvas.Brush.Style := bsClear;

  CheckListBox1.Clear;
  CheckListBox2.Clear;
  try
    for i := 1 to cnt do
      clients[i].Free;
  except
  end;

  for i := 1 to count do
  begin
    CheckListBox1.Items.add('Istemci-' + inttostr(i));
    CheckListBox1.Checked[CheckListBox1.Items.Count-
1]:=true;
    clients[i] := TShape.Create(Self);
    clients[i].Shape := stEllipse;
    clients[i].Brush.color := $000000CE;
    clients[i].Height := 10;
    clients[i].Width := 10;
    clients[i].Top := random(Image1.Height - 2 * radius -
clients[i].Height) + radius + 1;
    clients[i].Left := random(Image1.Width - 2 * radius -
clients[i].Width) + radius + 1;
    clients[i].Parent := Form1;
    x := clients[i].Top + clients[i].Height div 2;
    y := clients[i].Left + clients[i].Width div 2;
    DrawCircle(y, x, 50, clBlue, Image1, i);
    route[i].dx := random(10) + 5;
    route[i].dy := random(10) + 5;
  end;
  for i := 1 to count-1 do
  for j := i+1 to count do
  begin
   CheckListBox2.Items.add( IntToStr(i)+' and
'+IntToStr(j));
   CheckListBox2.Checked[CheckListBox2.Items.Count-
1]:=true;
  end;
end;

procedure TForm1.DrawCircle(x, y, r: integer; color:
TColor; image: TImage;
  clientindex: integer);
```

Ek-1 (Devamı). Delphi kodları

```
begin
  image.Canvas.pen.color := color;
  image.Canvas.pen.Style := psDashDotDot;
  image.Canvas.Ellipse(x - r, y - r, x + r, y + r);
  if clientindex <> 0 then
    image.Canvas.TextOut(x + 3, y + 3,
inttostr(clientindex));
end;

procedure TForm1.Timer1Timer(Sender: TObject);
var
  i, j,k, x, y, x1, y1, x2, y2: integer;
begin
  Image1.Canvas.Brush.color := clBtnFace;
  Image1.Canvas.FillRect(Canvas.ClipRect);
  Image1.Canvas.pen.color := color;
  Image1.Canvas.pen.Width := 1;
  Image1.Canvas.pen.Style := psDashDotDot;
  Image1.Canvas.Brush.Style := bsClear;

  for i := 1 to count do
  begin
    Image1.Canvas.FillRect(Canvas.ClipRect);

    if (clients[i].Left + radius > Image1.Width) or
(clients[i].Left < radius)then
      route[i].dx := -route[i].dx;

    if (clients[i].Top + radius > Image1.Height) or
(clients[i].Top < radius)then
      route[i].dy := -route[i].dy;

    clients[i].Left := clients[i].Left + route[i].dx;
    clients[i].Top := clients[i].Top + route[i].dy;

    x := clients[i].Top + clients[i].Height div 2;
    y := clients[i].Left + clients[i].Width div 2;

    DrawCircle(y, x, radius, clBlue, Image1, i);
  end;

  // Draw Acces Point
  x := AccessPoint.Top + AccessPoint.Height div 2;
  y := AccessPoint.Left + AccessPoint.Width div 2;
  DrawCircle(y, x, StrToInt(LabeledEdit5.Text), clNavy,
Image1, 0);
```

Ek-1 (Devamı). Delphi kodları

```
  Image1.Canvas.pen.color := clGreen;
  Image1.Canvas.pen.Style := psDot;
  // draw line between nodes
  k:=0;
  for i := 1 to count - 1 do
  for j := i + 1 to count do
    begin
      x1 := clients[i].Top + clients[i].Height div 2;
      y1 := clients[i].Left + clients[i].Width div 2;
      x2 := clients[j].Top + clients[j].Height div 2;
      y2 := clients[j].Left + clients[j].Width div 2;

      if sqr(x1 - x2) + sqr(y1 - y2) < sqr(radius) then
      if CheckListBox2.Checked[k] then
      begin
        Image1.Canvas.MoveTo(y1, x1);
        Image1.Canvas.LineTo(y2, x2);
      end;
      inc(k);
    end;

  // draw line between node and AP
  for i := 1 to count do
  begin
    x1 := clients[i].Top + clients[i].Height div 2;
    y1 := clients[i].Left + clients[i].Width div 2;
    x2 := AccessPoint.Top + AccessPoint.Height div 2;
    y2 := AccessPoint.Left + AccessPoint.Width div 2;
    if sqr(x1 - x2) + sqr(y1 - y2) < sqr(radius2) then
  // in area AP
    begin
      if not auth[i] then
      begin
        auth[i] := true;
        AuthenticateWithAP(i, CheckBox1.Checked);
      end
      else if CheckListBox1.Checked[i - 1] then
      begin
        Image1.Canvas.MoveTo(y1, x1);
        Image1.Canvas.LineTo(y2, x2);
      end;
    end
    else
      auth[i] := false;
  end;
end;
```

Ek-1 (Devamı). Delphi kodları

```
procedure TForm1.AuthenticateWithAP(clientindex: integer;
showmsg: boolean);
var
  i, j: integer;
begin
  i := clientindex;
  begin
    x1 := clients[i].Top + clients[i].Height div 2;
    y1 := clients[i].Left + clients[i].Width div 2;

    x2 := AccessPoint.Top + AccessPoint.Height div 2;
    y2 := AccessPoint.Left + AccessPoint.Width div 2;

    x3 := RadiusServer.Top + RadiusServer.Height div 2;
    y3 := RadiusServer.Left + RadiusServer.Width div 2;

    if showmsg then
      Memo1.lines.add('---ISLEMLER BASLIYOR---');

    DrawMessage(x1, y1, x2, y2, clGray, 'Istemci-' +
inttostr(i) + ' Starts',
      showmsg); // Start ((from client to AP))

    x1 := clients[i].Top + clients[i].Height div 2;
    y1 := clients[i].Left + clients[i].Width div 2;
    DrawMessage(x2, y2, x1, y1, clRed,
      'EN Istemciye Dogrulama Talebi Gonderir-' +
inttostr(i) + '', showmsg);
    // Request Identity (from AP to client)

    x1 := clients[i].Top + clients[i].Height div 2;
    y1 := clients[i].Left + clients[i].Width div 2;
    DrawMessage(x1, y1, x2, y2, clGray, 'Istemci-' +
inttostr(i)
        + 'Dogrulama Bilgilerini Gonderir', showmsg); //
Identity (from client to AP)

    DrawMessage(x2, y2, x3, y3, clBlue, 'EN Dogrulama
Bilgilerini RS`e Gonderir', showmsg);
    // Identity (from AP to RadiusServer)

    if showmsg then
      Memo1.lines.add('---RADIUS SUNUCU ISTEMCIYI
DOGRULAR---');

    if CheckListBox1.Checked[i - 1] = true then
```

Ek-1 (Devamı). Delphi kodları

```
      DrawMessage(x3, y3, x2, y2, clGreen,
        'RS EN`na kimlik dogrulama onay mesajini
gonderir' + 'Istemci-' + inttostr
          (i) + '', showmsg) // from RS to AP
    else
      DrawMessage(x3, y3, x2, y2, clGreen,
        'RS EN`na kimlik dogrulama reddi mesajini
gonderir Istemci-' + inttostr(i)
          + '', showmsg); // from RS to AP

    x1 := clients[i].Top + clients[i].Height div 2;
    y1 := clients[i].Left + clients[i].Width div 2;
    if CheckListBox1.Checked[i - 1] = true then

      DrawMessage(x2, y2, x1, y1, clRed,
        'EN kimlik dogrulama onay mesajini gonderir
Istemci-' + inttostr(i) + '',
        showmsg) // from AP to client
    else
      DrawMessage(x2, y2, x1, y1, clRed,
        'EN kimlik dogrulama reddi mesajini gonderir
Istemci-' + inttostr(i) + '',
        showmsg); // from AP to client

    x1 := clients[i].Top + clients[i].Height div 2;
    y1 := clients[i].Left + clients[i].Width div 2;
    DrawMessage(x1, y1, x2, y2, clGray, 'Istemci-' +
inttostr(i) +
        ' EN`na kimlik dogrulama mesajina tekrar yanit
gonderir', showmsg);
    // from client to AP

    DrawMessage(x2, y2, x3, y3, clBlue,
      'EN kimlik dogrulamaya tekrar yanit mesajini RS`ya
gonderir', showmsg); // from AP to RS

    if CheckListBox1.Checked[i - 1] = true then
    begin
      if showmsg then
        Memo1.lines.add('---ISTEMCI-' + inttostr(i) +
            ' RADIUS SUNUCUSUNU DOGRULAR---');

      x1 := clients[i].Top + clients[i].Height div 2;
      y1 := clients[i].Left + clients[i].Width div 2;
```

Ek-1 (Devamı). Delphi kodları

```
      DrawMessage(x1, y1, x2, y2, clGray, 'Istemci-' +
inttostr(i) + ' EN`na kimlik dogrulama mesaji gonderir',
showmsg); // from client to AP

      DrawMessage(x2, y2, x3, y3, clBlue, 'EN RS`ya
kimlik dogrulama mesajini gonderir',
        showmsg); // from AP to RS

      if showmsg then
      begin
        Memo1.lines.add('RS OTURUM ANAHTARI olusturur');
        // create session key for RS
        SessionKey := '';
        for j := 1 to 32 do
        SessionKey := SessionKey + chr(random(30) + 97);
        Memo1.lines.add('Olusturulan OTURUM ANAHTARI: ' +
SessionKey);
      end;

      DrawMessage(x3, y3, x2, y2, clGreen,
        'RS EN`na kimlik dogrulama mesajini gonderir',
showmsg); // from RS to AP

      x1 := clients[i].Top + clients[i].Height div 2;
      y1 := clients[i].Left + clients[i].Width div 2;
      DrawMessage(x2, y2, x1, y1, clRed,
        'EN kimlik dogrulama mesajini gonderir Istemci-'
+ inttostr(i) + '', showmsg);
      // from AP to client

      if showmsg then
  Memo1.lines.add('Istemci RS`den GRUP ANAHTARINI alir');

      // create broadcast key
        BroadcastKey := '';
        for j := 1 to 32 do
          BroadcastKey := BroadcastKey + chr(random(30) +
97);
        Keylength := 32;
        if showmsg then
          Memo1.lines.add('Olusturulan GRUP ANAHTARI: ' +
BroadcastKey);
```

Ek-1 (Devamı). Delphi kodları

```
      if RadioGroup1.ItemIndex = 0 then
      begin
        // Encrypring with RC4=========================
        s := BroadcastKey;
        setlength(s1, length(s));
        RC4Init(RC4, SessionKey);
        RC4Code(RC4, s[1], s1[1], length(BroadcastKey));
        RC4Done(RC4);
        EncyrptedKey := s1;
      end;
      if RadioGroup1.ItemIndex = 1 then
      begin
        // Encrypring with DES=========================
        setlength(Data, 0);
        j := 1;
        While j <= length(BroadcastKey) Do
        Begin
          s := Copy(BroadcastKey, j, 8);
          Data := ConcatBits([Data, DESEncode(s,
SessionKey)]);
          j := j + 8;
        End;
        EncyrptedKey := BinToAnsiStr(Data);
        // end Encryption==============================
      end;

      DrawMessage(x2, y2, x1, y1, clRed,
        'EN sifreli GRUP ANAHTARINI gonderir Istemci-' +
inttostr(i) + '',
        showmsg);
      if showmsg then
        Memo1.lines.add('SIFRELI GRUP ANAHTARI: ' +
EncyrptedKey);

      DrawMessage(x2, y2, x1, y1, clRed,
        'EN ANAHTAR UZUNLUGUNU gonderir Istemci-' +
inttostr(i) + '', showmsg);
      if showmsg then
      begin
        Memo1.lines.add('ANAHTAR UZUNLUGU: ' +
inttostr(Keylength));
        Memo1.lines.add('Istemci-' + inttostr(i) +
            ' GRUP ANAHTARINI OTURUM ANAHTARI ile desifre
eder');
```

Ek-1 (Devamı). Delphi kodları

```
        if RadioGroup1.ItemIndex = 0 then
        begin
          // Decrypring with RC4=========================
          s := EncyrptedKey;
          setlength(s1, length(s));
          RC4Init(RC4, SessionKey);
          RC4Code(RC4, s[1], s1[1],length(EncyrptedKey));
          RC4Done(RC4);
          BroadcastKey := s1;
        end;
        if RadioGroup1.ItemIndex = 1 then
        begin
          // Decrypring with DES=======================
          setlength(Data, 0);
          j := 1;
          While j <= length(EncyrptedKey) Do
          Begin
    Data := ConcatBits([Data,
DESDecode(Copy(EncyrptedKey, j, 8), SessionKey)]);
            j := j + 8;
          End;
          BroadcastKey := BinToAnsiStr(Data);
        end;
        Memo1.lines.add('Desifre edilmis GRUP ANAHTARI: '
+ BroadcastKey);

        Memo1.lines.add('KIMLIK DOGRULAMA BASARIYLA
GERCEKLESTIRILDI Istemci-' + inttostr(i)
            + '');
      end;
    end
    else if showmsg then
    begin
      Memo1.lines.add('KIMLIK DOGRULAMA
GERCEKLESTIRILEMEDI Istemci-' + inttostr(i) + '');
      Memo1.lines.add('');
    end;
  end;
end;

procedure TForm1.Button3Click(Sender: TObject);
begin
  Timer1.Enabled := false;
end;

end.
```

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı	: BABAYEV, Rustam
Uyruğu	: Azerbaycan
Doğum tarihi ve yeri	: 27.04.1986 Bakü/AZERBAYCAN
Medeni hali	: Bekar
Telefon	: (+99450) 682 36 37, (+90505) 863 46 01
E-mail	: rustam_babayev@rambler.ru

Eğitim

Derece	Eğitim Birimi	Mezuniyet tarihi
Yüksel lisans	Gazi Üniversitesi/Bilişim Enstitüsü/ Bilgisayar Bilimleri	2011
Lisans	Bakü Devlet Üniversitesi/ Uygulamalı Matematik ve Bilgisayar	2006
Lise	158 No.lu Okul, Bakü/AZERBAYCAN	2002

İş Deneyimi

Yıl	Yer	Görev
2010 –	Azerbaycan Cumhuriyeti Maliye Bakanlığı	Yönetici danışman (Bilişim Teknolojileri)

Yabancı Dil

İngilizce, Rusça

İlgi alanları ve hobiler

Bilgisayar teknolojileri, kriptografi, klasik müzik, piyano, bilardo, sudoku, aikido, felsefe, bilgi yarışmaları, satranç, zeka testleri vs.