Kablosuz Ağlarda Güvenlik

Takdim

- Giriş
- Kablosuz Ağların Taşıdığı Riskler
- Güvenlik Yöntemleri ve Protokolleri
- Servis Seti Tanımlayıcı (SSID-Service Set Identifier)
- MAC Adresi ile Doğrulama
- Kabloluya Eşdeğer Gizlilik (WEP-Wired Equivalent Privacy)
- Wİ-Fİ Korumalı Erişim (WPA-Wi-fi Protected Access)
- 802.11i(RSN-Robust Security Network, WPA2)

Giriş

- Kablosuz ağlarda veriler radyo dalgalarıyla havadan üretilir.
- İletişimin lisanssız frekans bantlarında yapılması, kablosuz ağların istenmeyen kişiler tarafından fark edilmesini sağlamaktadır.

Kablosuz Ağların Taşıdığı Riskler

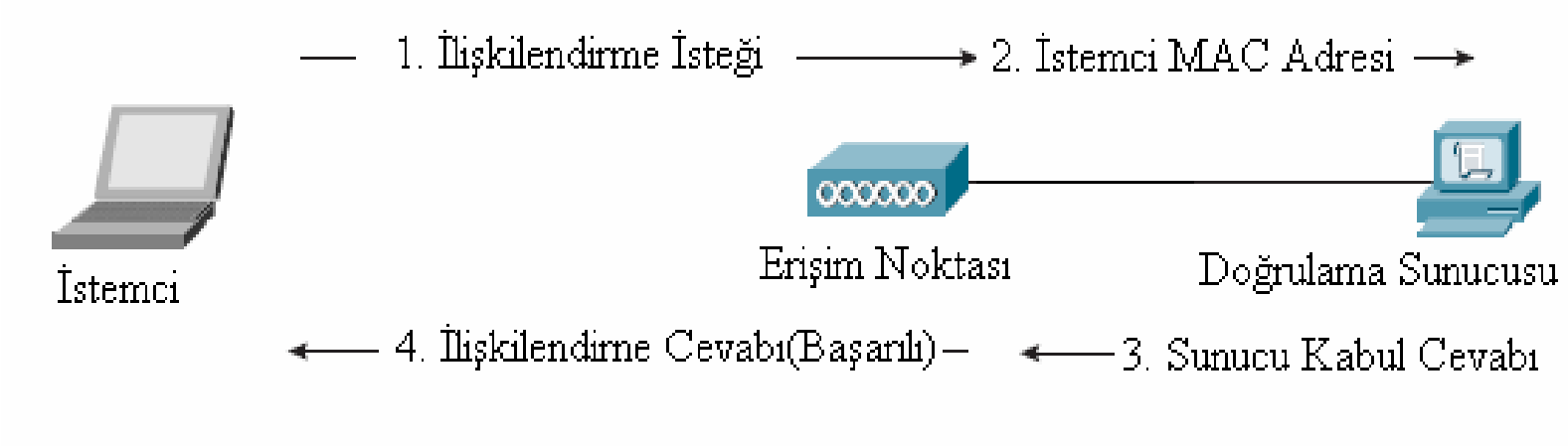
- Kablolu ağa sızma
- Trafiğin dinlenip verinin çözümlenmesi
- Ağ topolojisinin ortaya çıkması
- İstemcilerin yetkisiz erişim noktalarına bağlanması
- İstenmeyen yerlere servis verme
- Servis dışı bırakma(DoS)

Güvenlik Yöntemleri ve Protokolleri

- Bu kapsamda kablosuz ağlarda güvenliği sağlamak için aşağıdaki kriterlerin sağlanması gerekmektedir.
  - Asıllama: Kimlik bilgilerinin geçerliliğinin denetlenmesi.
  - Şifreleme:Veri paketleri gönderilmeden önce, gizliliğin sağlanması için veriler şifrelenmelidir.
  - Veri Bütünlüğü: Veri paketi gönderilmeden önce, gerek alıcı gerek verici tarafından iletinin içeriğini kontrol eden ve sıralayan bir bilgi iletiye eklenmelidir.

MAC Adresi ile Doğrulama

- Her erişim noktasının geçerli bir erişim kontrol listesine ihtiyaç duyarlar.
- Kullanıcının ağı kullanması bu erişim kontrol listesine göre yapılır.



MAC Adresi ile Doğrulama

Zayıflıkları

- MAC adreslerini kullanarak kontrol etmek, takibi zor bir iştir.
- MAC adresleri iletilirken şifresizdir.
- Hiçbir zaman kablosuz güvenlik sağlamanın ana metodu olmamalıdır. (MAC adresini güvenilir bir MAC adresi ile değiştirebilir.)

Kabloluya Eşdeğer Gizlilik (WEP-Wired Equivalent Privacy)

- 802.11 standardıyla beraber geliştirilmiş olan temel güvenlik birimidir.
- Teknik alt yapısı RC4 (Rivest Cipher) akış şifreleme algoritmasına dayanır.

Kabloluya Eşdeğer Gizlilik (WEP-Wired Equivalent Privacy)

- İlgili standart kimlik doğrulama için iki seçenek sunmaktadır.
  - Açık Sistem Kimlik Doğrulama
  - Paylaşılan Anahtar ile Kimlik Doğrulama

Kabloluya Eşdeğer Gizlilik (WEP-Wired Equivalent Privacy)

Açık Sistem Kimlik Doğrulama

- Gerçekte herhangi bir kimlik doğrulama yapılmamaktadır.
- Erişim noktasına kablosuz ağ bağdaştırıcının MAC adresi gönderilmektedir.
- Erişim noktası bilgiyi kaydederek istemciye kablosuz erişim hakkı verir.

Kabloluya Eşdeğer Gizlilik (WEP-Wired Equivalent Privacy)

Paylaşılan Anahtar ile Kimlik Doğrulama

- Ortak bir anahtar tutulmaktadır.
- İstemci erişim noktasına rastgele bir mesaj yollar.
- İstemci bu mesajı ortak anahtar ile şifreleyip gönderir.
- Ortak anahtar ile şifrelendiğini doğrularsa izin verir.
- Ortak anahtar aynı zamanda şifreleme amaçlı da kullanılmaktadır. Bu da şifreleme kısmı için güvenlik açığı ortaya çıkarmaktadır.

Kabloluya Eşdeğer Gizlilik (WEP-Wired Equivalent Privacy)

Şifreleme

- Şifreleme için RC4 şifreleme algoritması istemcilerde ve erişim noktaları üzerinde girilen ortak anahtar ile kullanılmaktadır.
- İstemci ve erişim noktası tarafında 40 bitlik statik bir anahtar tanımlanır.
- Akış şifresini elde etmek için 24 bitlik IV (Initializition Vector-Başlangıç Vektörü) kullanılır.

Kabloluya Eşdeğer Gizlilik (WEP-Wired Equivalent Privacy)

Veri Bütünlüğü

- 32 bit CRC (Cyclic Redundancy Check)' e dayanan ICV (Integrity Check Value) kullanılmaktadır.
- Veri paketini 32-bit CRC'si oluşturulmakta ve WEP anahtarı ile şifrelenerek alıcıya gönderilmektedir.
- ICV kriptografik veri bütünlüğü sunmamaktadır.
- Bu sebep ile bit değiştirme ve tekrarlama saldırılarına karşı konulamamaktadır.

Kabloluya Eşdeğer Gizlilik (WEP-Wired Equivalent Privacy)

Veri Bütünlüğü

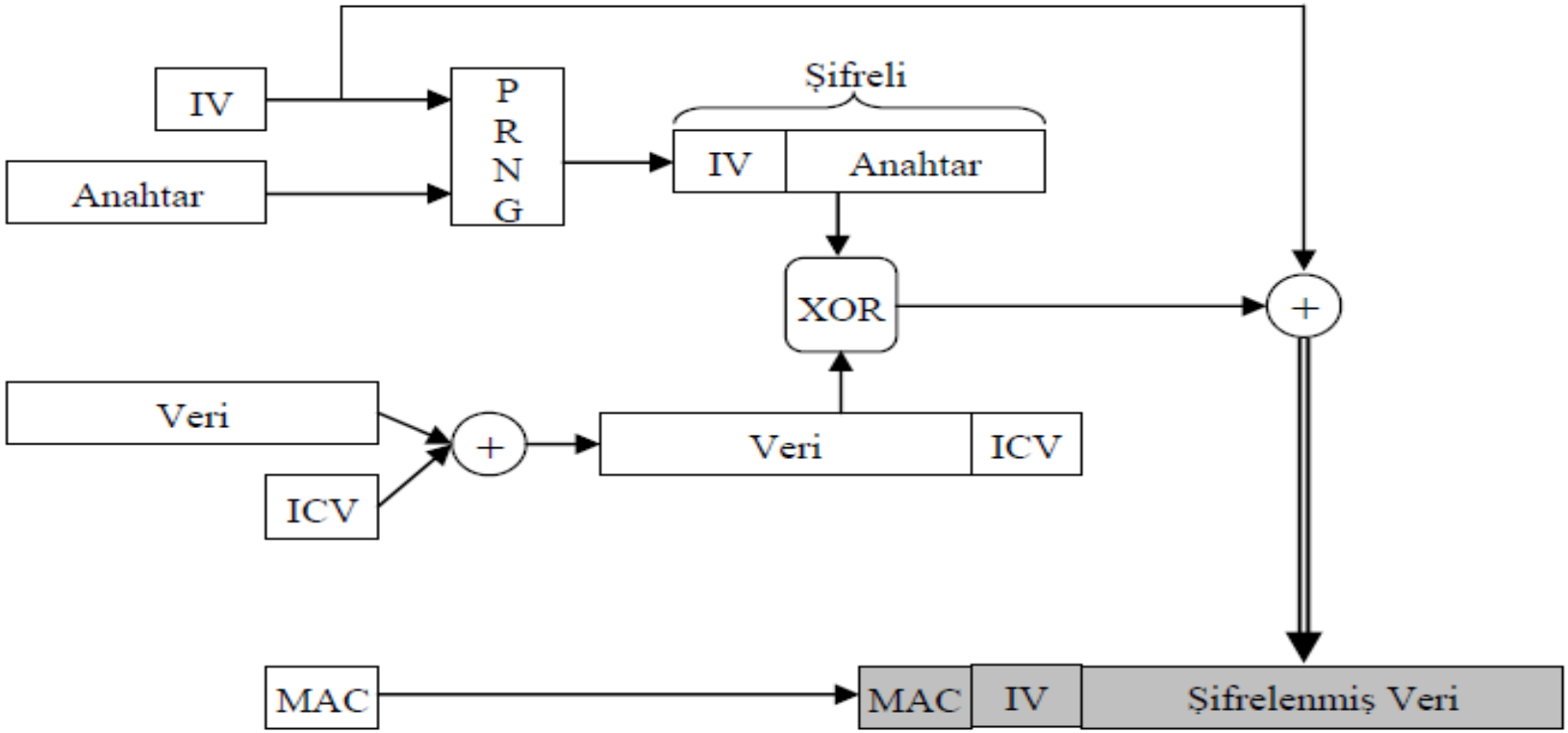
- Bit değiştirme saldırısında, şifreli mesajın belli bitleri değiştirilip şifreli ICV'de de karşılık gelen değişiklik ortak anahtar bilinmeden yapılabilmektedir.
- Tekrarlama saldırılarında ise saldırgan tarafından yakalanmış bir paket farklı bir zaman da erişim noktasına veya istemciye gönderilebilmektedir.
- Bu sayede kripto analiz için yapay veri trafiği oluşturulabilmektedir.
- Erişim noktaları tekrarlanan paketlere yanıt paketleri göndermektedir.

Kabloluya Eşdeğer Gizlilik (WEP-Wired Equivalent Privacy)

WEP Çalışma Şekli

1. Veri bütünlüğünü sağlamak amacıyla, veri bir doğrulama algoritmasına tabi tutularak, doğrulama bitleri elde edilir.
2. Doğrulama bitleri verinin sonuna eklenir.
3. 24 bitlik IV statik anahtarın başına eklenir.
4. 64 bitlik paket RC4 algoritması ile şifrelenir.
5. Elde edilen veriler XOR işleminden geçer.
6. Elde edilen verinin başına IV eklenir ve iletilecek şifreli veri elde edilir.
7. Elde edilen bu verinin başına, alıcı ve verici MAC adresleri eklenerek kablosuz ortama gönderilir.
8. Şifreli veri, karşı tarafta aynı işlemlerin tersi yönde uygulanarak açılır.

Kabloluya Eşdeğer Gizlilik (WEP-Wired Equivalent Privacy)



Kabloluya Eşdeğer Gizlilik (WEP-Wired Equivalent Privacy)

Zayıflıkları

- Ortak anahtar, herhangi bir şekilde istenmeyen bir kişi tarafından elde edilebilinir. Ortak anahtara sahip olan ağı istediği gibi kullanabilmektedir.
- WEP'te tekrar saldırıları için herhangi bir güvenlik önlemi yoktur. Aynı mesaj defalarca gönderilebilinir ve bu alıcı tarafından anlaşılmaz. Sisteme giriş yapan bir kullanıcı sistemden çıktıktan sonra dinlenilen mesajlar doğrulayıcıya gönderilirse araya giren kişi, mesaj içeriğini bilmese de kendini doğrulatabilir.

Kabloluya Eşdeğer Gizlilik (WEP-Wired Equivalent Privacy)

Zayıflıkları

- Bit değiştirme zayıflığı ICV bütünlük kontrol verisinin oluşturma şeklinden kaynaklanmaktadır.
- ICV lineer bir metotla oluşturulup asıl verinin sonuna eklenip şifrelenmektedir.
- Bundan dolayı veri alanında bir değişiklik yapıldığında ICV de oluşacak değişiklik hesaplanabilmektedir.

Kabloluya Eşdeğer Gizlilik (WEP-Wired Equivalent Privacy)

Zayıflıkları

1. Saldırgan dinlediği ağdan bir paket alır.
2. Dinlediği paketteki veri ve ICV alanlarını değiştirir.
3. Bu paketi ağa gönderir.
4. Erişim noktası ICV değerini kontrol edip çerçeveyi gönderir.
5. Burada CRC kontrol edilir ve belirli edilen bir hata döndürülür.
6. Erişim noktası bu hatayı şifreler ve gönderir.
7. Araya giren belirli hatanın hem şifreli hem de açık metnine sahip olur.
8. XOR işlemi ile buradan akış şifresini elde eder.

Kabloluya Eşdeğer Gizlilik (WEP-Wired Equivalent Privacy)

Zayıflıkları

- IV tekrar kullanılması bir başka zayıflığıdır.
- RC4 algoritması parametre olarak ortak anahtar ile IV'ü geçirmektedir.
- IV değeri her paket için değişmektedir.
- 24 bit uzunluktaki IV 224 farklı değer alır.
- Böylece RC4 algoritmasından 224 tane farklı akış şifresi elde edilmiş olunur.
- Dolayısıyla 224 paket sonra aynı IV değeri tekrar kullanılacaktır.
- Ağı dinleyen bir saldırgan, tekrar eden bu verileri alarak istatistiksel yöntemler ile veriyi deşifre eder.

Kabloluya Eşdeğer Gizlilik (WEP-Wired Equivalent Privacy)

Zayıflıkları

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

Kabloluya Eşdeğer Gizlilik (WEP-Wired Equivalent Privacy)

Zayıflıkları

- WEP anahtar ile kimlik doğrulama tek yönlü bir kimlik doğrulama yöntemidir.
- İstemci erişim noktası tarafından doğrulanmakta fakat erişim noktası istemci tarafından doğrulanmamaktadır.
- Bir saldırgan yakınlara bir noktaya erişim noktası ekleyip normal ağın işleyişini etkileyebilir.
- İstemciler güvenilir erişim noktasına bağlandığından emin olmaz.

Kabloluya Eşdeğer Gizlilik (WEP-Wired Equivalent Privacy)

Yeni Uyarlamalar Geliştirilmiştir

- IV 24 bitten 128 bite çıkarılmıştır.
- Ortak anahtar uzunluğu 40 bitten 104 bitte uzatılmıştır.
- Bu yenilikler WEP'in mevcut açıklıklarını gidememiştir.

Wİ-Fİ Korumalı Erişim (WPA-Wi-fi Protected Access)

- WEP standardında bulunan açıklıkların ortaya çıkmasıyla birlikte IEEE yeni bir güvenlik standardı(IEEE 802.11i) oluşturmak amacıyla çalışmalara başlamıştır.
- Ara çözüm olarak WPA standardını oluşturmuştur.

Wİ-Fİ Korumalı Erişim (WPA-Wi-fi Protected Access)

Kimlik Doğrulama

- Kimlik Doğrulama için iki seçenek sunmaktadır.
  - WPA-PSK
  - 802.1x

Wİ-Fİ Korumalı Erişim (WPA-Wi-fi Protected Access)

WPA-PSK

- Ev ve küçük işletmeler için tasarlanmıştır.
- Kimlik doğrulama için istemciler ve erişim noktası üzerinden girilen bir paylaşılan parola (PSK) kullanılmaktadır.
- Paylaşılan anahtar istemcilerin işletim sisteminde tutulmaktadır ve bu sebeple anahtarın başkalarının eline geçme riski vardır.
- Kimlik doğrulama trafiğini kaydeden saldırganların sözlük saldırılarına olanak tanıyan bir yapıdır.

Wİ-Fİ Korumalı Erişim (WPA-Wi-fi Protected Access)

WPA-PSK

- Tek anahtar kullanımı kullanıcıların ayırt edilebilmesini/farklı yetkilendirmelerin yapılmasını/kullanıcı tabanlı kayıt tutulmasını olanaksız kılmaktadır.
- Bir istemci bilgisayarın çalınması durumunda yada yetkisiz bir erişim olduğunda PSK' nın ele geçmesi muhtemeldir.
- Kurumsal kablosuz ağlarda kullanımı uygun değildir.

Wİ-Fİ Korumalı Erişim (WPA-Wi-fi Protected Access)

802.1x

- Port tabanlı ağ erişim kontrol mekanizmasıdır.
- PEAP(Kullanıcı hesap bilgilerini kullanarak), EAP-TLS(Sertifika tabanlı), EAP-MD5(şifre kullanarak) vb. protokoller kullanarak kimlik doğrulama işlemi gerçekleştirebilmektedir.
- Çift yönlü kimlik doğrulama mümkündür. İstemciler ve sunucu karşılıklı olarak kimlik doğrulama işlemi gerçekleştirebilirler.

Wİ-Fİ Korumalı Erişim (WPA-Wi-fi Protected Access)

802.1x

- 802.1x ile yetkilendirmede erişim politikaları tanımlanabilmekte, ait olduğu etki alanı, kullanıcı grubu, bağlantı türü, bağlantı zamanı, bağlandığı erişim noktası gibi kriterlere göre yetkilendirme yapabilmektedirler.

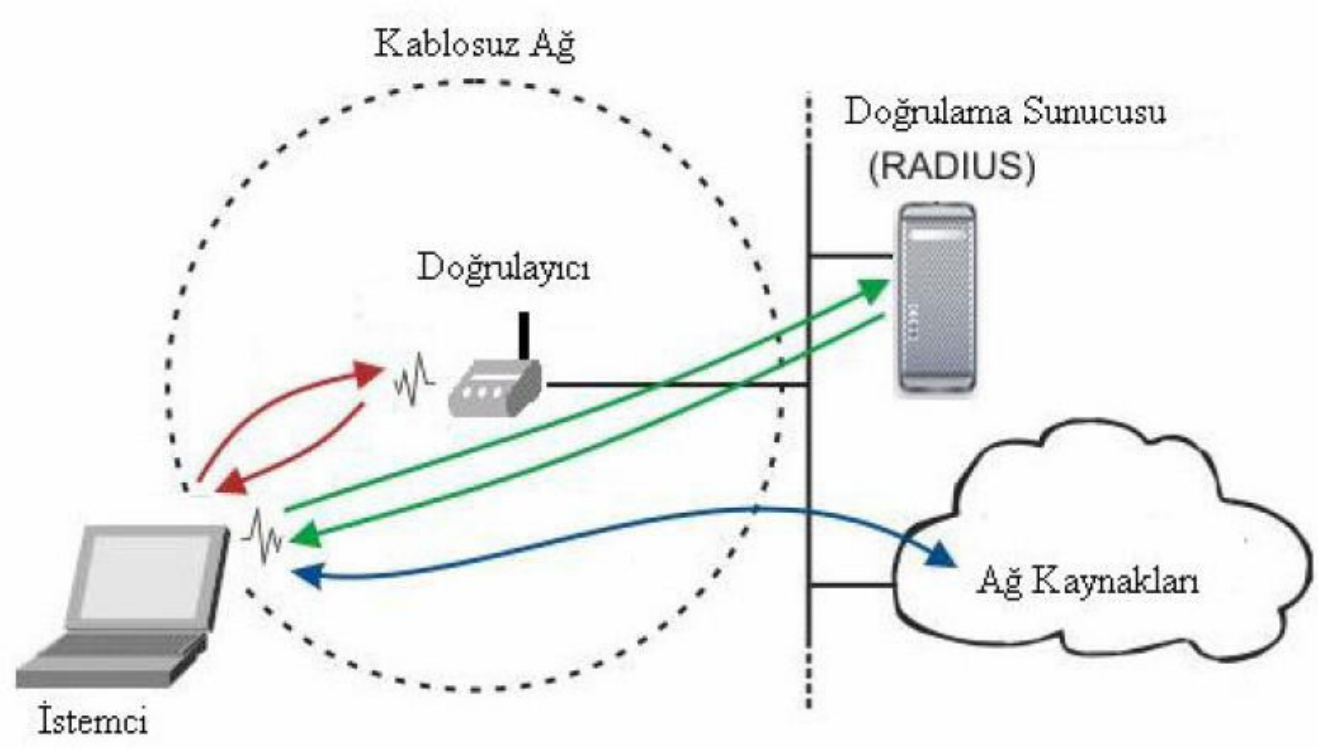
Wİ-Fİ Korumalı Erişim (WPA-Wi-fi Protected Access)

802.1x ile Kimlik Doğrulama

1. İstemci doğrulayıcıya bağlantı talebinde bulunur.
2. Doğrulayıcı bağlantı isteğini alınca, tüm portları kapalı tutar, sadece istemci ile arasında bir port açar.
3. Doğrulayıcı, kullanıcıdan kimliğini ister. İstemci kimliğini gönderir, doğrulayıcı kimlik bilgisini doğrulama sunucusuna gönderir. Kimlik gönderildikten sonra kimlik kanıtlama süreci başlar. Sunucu kimliği doğrular ve doğrulayıcıya gönderir. Doğrulayıcı, istemcinin portunu yetkilendirilmiş duruma getirir.
4. İstemci doğrulama sunucusundan, onun kimliğini ister. Doğrulama sunucusu, kimlik bilgisini istemciye gönderir.
5. İstemci, doğrulama sunucusunun kimliğini doğruladığında, veri trafiğine başlanır.

Wİ-Fİ Korumalı Erişim (WPA-Wi-fi Protected Access)

802.1x ile Kimlik Doğrulama



Wİ-Fİ Korumalı Erişim (WPA-Wi-fi Protected Access)

Şifreleme

- Şifreleme için Geçici Anahtar Bütünlüğü Protokolü(Temporal Key Integrity Protocol-TKIP) kullanılmaktadır.
- TKIP yapısında RC4 kullanmakta, fakat WEP'ten farklı olarak her bir pakette şifreleme anahtarı değiştirilmekte ve IV uzunluğu 24 bit yerine 48 bittir.
- IV aynı zaman da paketlere sıra numarası vermek içinde kullanılır. Böylece tekrar saldırıları önlenir. Ayrıca sırasız gelen paketler alıcı tarafından atılmaktadır.
- WEP'ten TKIP'a donanım değişikliği olmadan geçişe imkan verebilmek amacıyla RC4 kullanımına devam edilmiştir.

Wİ-Fİ Korumalı Erişim (WPA-Wi-fi Protected Access)

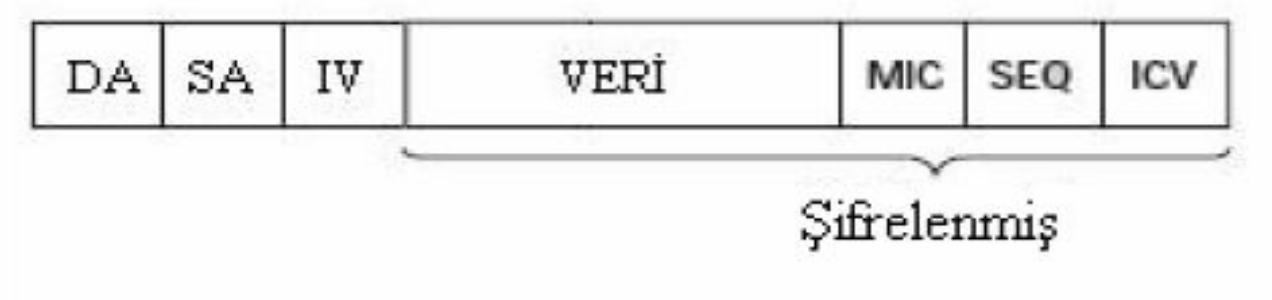
Veri Bütünlüğü

- WEP yapısından farklı olarak basit CRC hesaplaması yerine kriptografik veri bütünlüğü kontrolü yapılmasına olanak sağlamaktadır.
- Tekrarlama, bit değiştirme saldırılarına karşı WEP'in taşıdığı zayıflıkları taşımaz.
- Veri bütünlüğü için Michael olarak adlandırılan, paketlerin veri kısmı özetinin(hash) TKIP ile şifrelenmesi yöntemi kullanılmaktadır.
- Veri bütünlüğü için kullanılan anahtar, veri şifreleme anahtarından farklıdır ve 802.1x kimlik doğrulama aşamasında oluşturulmaktadır.

Wİ-Fİ Korumalı Erişim (WPA-Wi-fi Protected Access)

Michael Veri Bütünlük Kodu(MIC-Message Integtiry Code)

- Alıcı ve gönderen MAC adresleri ve mesaj bir anahtarlama işlevi(hashing) fonksiyonuna tabi tutulur ve 8 baytlık bir çıktı oluşur.
- MIC bilgisi 802.11 veri çerçevesinin veri alanı ile ICV bilgisi arasına yerleştirlir.
- MIC alanı, veri ve ICV ile birlikte şifrelenir.



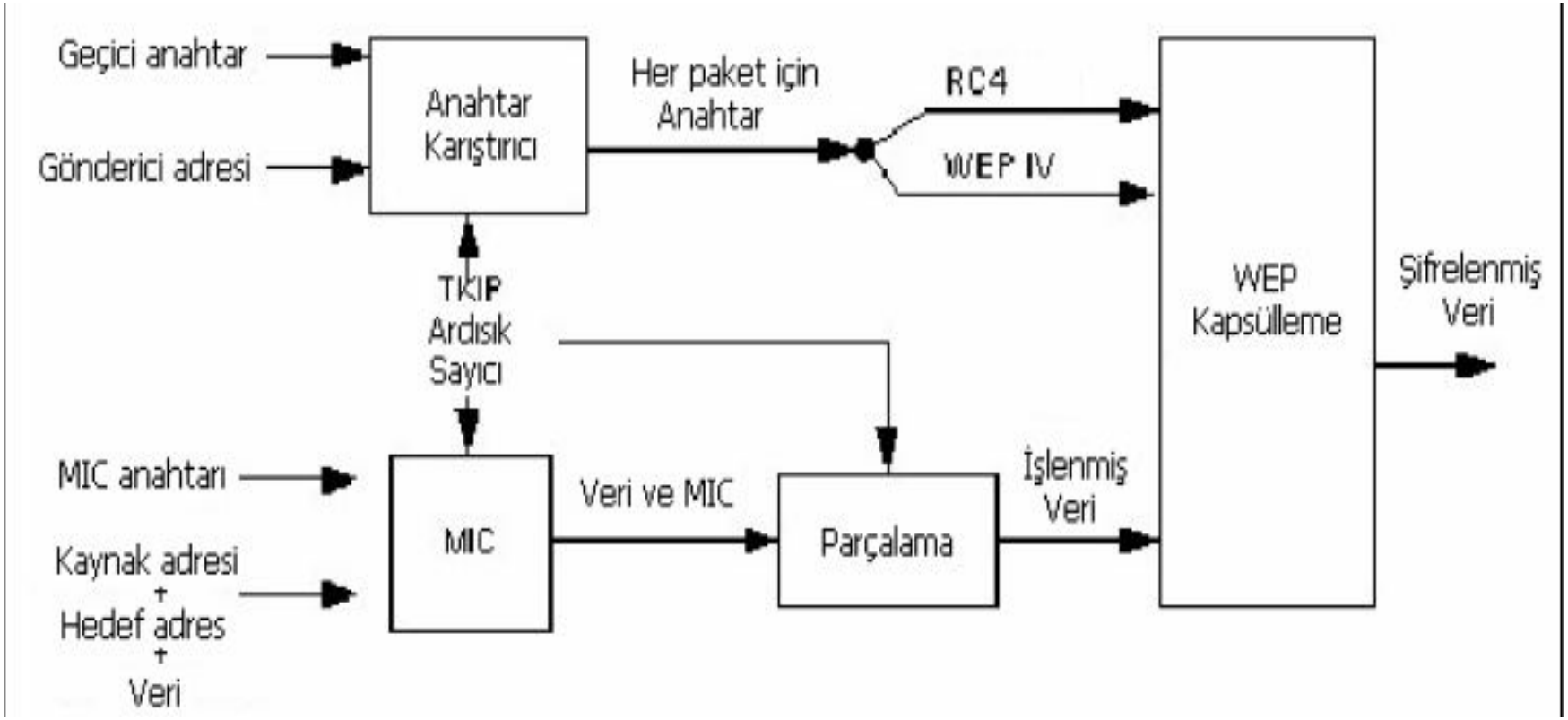
Wİ-Fİ Korumalı Erişim (WPA-Wi-fi Protected Access)

WPA Şifreleme Adımları

1. IV, DA ve veri şifreleme anahtarı bir WPA anahtar karıştırma fonksiyonuna girilerek her paket için şifreleme anahtarı hesaplanır.
2. DA, SA, veri, veri bütünlük anahtarı Michael veri bütünlük algoritmasına girerek MIC elde edilir.
3. IV ile şifreli her paket RC4 PRNG fonksiyonuna girerek, MIC ve ICV ile aynı veri genişliğindeki bir akış anahtarı üretilir.
4. Veri, MIC ve ICV kombinasyonu ile akış anahtarı XOR işlemine tabii tutularak şifrelenmiş metin elde edilir.

Wİ-Fİ Korumalı Erişim (WPA-Wi-fi Protected Access)

WPA Şifreleme Adımları



IEEE 802.11i-WPA2 (RSN-Robust Security Network)

- WEP'in zayıflıklarını tümüyle ortadan kaldırmak amacıyla oluşturulmuş güvenlik standardıdır.
- AES şifreleme algoritmasının Sayaç Modu ile Zincirleme Blok Şifreleme Mesaj Doğrulama Kodu (Counter Mode with Cipher Block Chaining Massage Authentication Code Protocol- CCMP) modunda şifreleme ve veri bütünlüğü kontrolü için, 802.1x'in kimlik doğrulama/yetkilendirme için kullanımını önermektedir.
- Gezginlik (roaming) sağlanır. Gerçek zamanlı iletişimlerde veri kaybını engeller.

IEEE 802.11i-WPA2 (RSN-Robust Security Network)

Kimlik Doğrulama/Yetkilendirme

- WPA ile aynı yapıyı, 802.1x'i kullanmaktadır.

IEEE 802.11i-WPA2 (RSN-Robust Security Network)

Şifreleme

- AES şifreleme algoritmasını Counter Mode modunda kullanılmaktadır.
- Bu yöntem ile her paket için tek kullanımlık anahtara ihtiyaç kalmaksızın şifreleme anahtarının tekrarını önleyen bir yapı oluşturulur.
- AES şifreleme algoritması RC4 algoritmasına göre daha güçlüdür.

IEEE 802.11i-WPA2 (RSN-Robust Security Network)

Veri Bütünlüğü

- WPA veri bütünlüğü kontrolünden farklı olarak paketlerin veri kısmı özetleri AES Zincirleme Blok Şifreleme Mesaj Doğrulama Kodu ile şifrelemektedir.

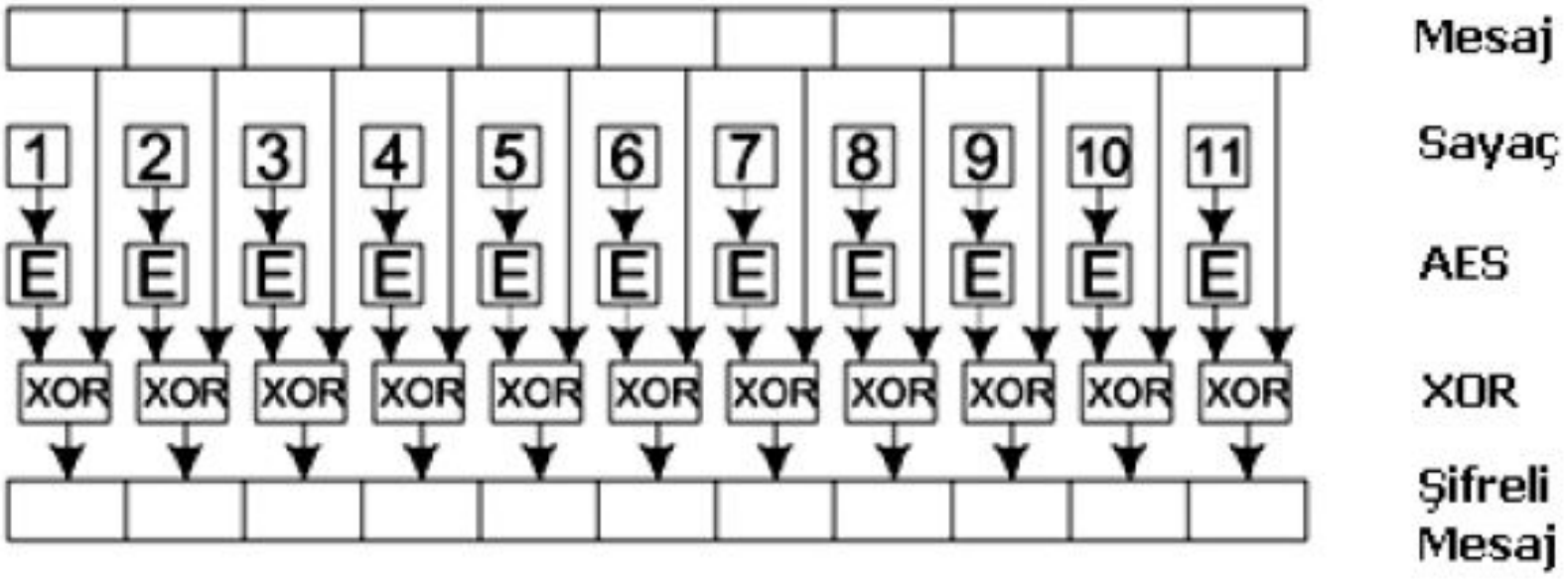
IEEE 802.11i-WPA2 (RSN-Robust Security Network)

Sayaç Modu (Counter Mode)

- Sayaç yönteminin kullanım amacı aynı veri içeren bloklar aynı şifre ile şifrelendiğinde farklı çıkışların olmasının istenmesidir.
- Çünkü mesajın tekrar eden bloklardan oluştuğunun bilinmesi bir zayıflıktır.
- Sayaç, keyfi fakat önceden belirlenmiş bir değerle, belirlenmiş bir usulde artmaya başlar.
- Gizliliği sağlamaktadır, veri bütünlüğünü sağlamaz.
- AES şifreleme, sayaç bir anahtar akışı ile şifrelendikten sonra yapılır.
- Daha sonra üretilen 128 bitlik bu blokla, 128 bitlik bloklara ayrılmış veri XOR işlemine tabi tutulur.
- Veri blokları şifrelenmiş sayılar ile XOR işlemine tutulmaktadır.
- Burada sayılar rastgele seçilmektedir çünkü aynı iki mesaj aynı çıkışları verecektir.
- Akış şifreleme tarafından işlenmiş blok şifrelemeye izin verir.
- Şifrenin çözülmesi için AES bloklarının bilinmesi yeterlidir.

IEEE 802.11i-WPA2 (RSN-Robust Security Network)

Sayaç Modu (Counter Mode)



IEEE 802.11i-WPA2 (RSN-Robust Security Network)

Zincirleme Blok Şifreleme Mesaj Doğrulama Kodu(CBC-MAC)

- 802.11i çalışma grubu veri bütünlüğünü sağlamak için kullanılır.
- CBC, bir mesaj bütünlük kodu (MIC) üretir.
- MIC şifrelenmiş bir mesaj doğrulama kodu oluşturur.

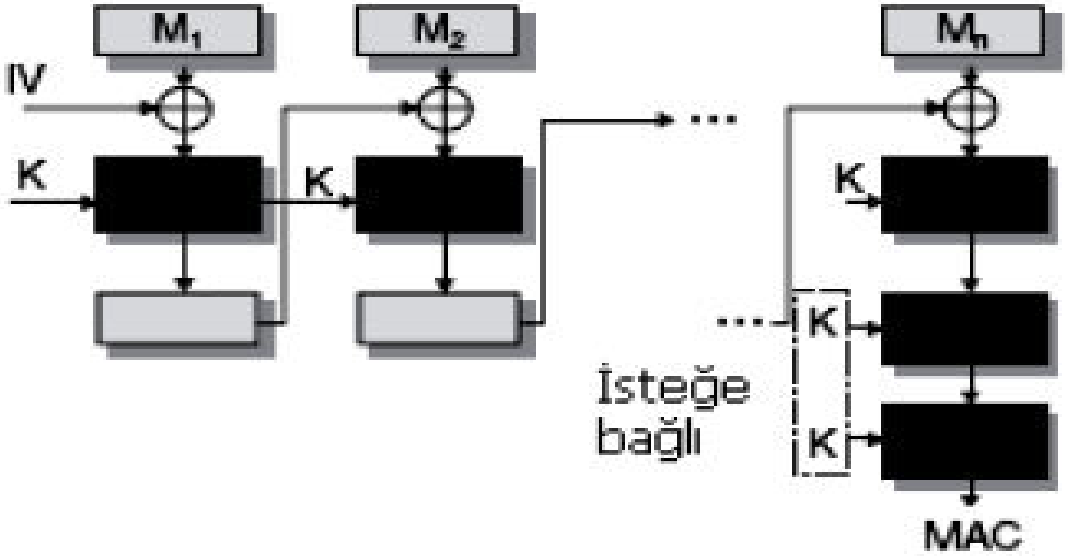
IEEE 802.11i-WPA2 (RSN-Robust Security Network)

Zincirleme Blok Şifreleme Mesaj Doğrulama Kodu(CBC-MAC)

- Mesajın ilk bloğu alınır IV ile XOR işlemine tabi tutulur ve bir anahtar ile AES kullanılarak şifrelenir.
- Sonuç, ikinci blok ile XOR işlemine tabi tutulur ve sonra elde edilen sonuç şifrelenir.
- Bu sonuç son blok kullanılana kadar devam eder. Sonuç olarak tek blok uzunluğunda şifrelenmiş bir veri oluşur.
- IV ve sayaç paketleri 128 bit uzunluğundadır.

IEEE 802.11i-WPA2 (RSN-Robust Security Network)

Zincirleme Blok Şifreleme Mesaj Doğrulama Kodu(CBC-MAC)



IEEE 802.11i-WPA2 (RSN-Robust Security Network)

- WPA2'de şifreleme işlemi Counter Mode ve CBC-MAC kullanılarak gerçekleştirilir.
- Bu iki yöntemin hepsine birden CCMP adı verilir.

Karşılaştırma

	WEP	WPA	RSN
Şifreleme	RC4 algoritması (Şifreleme yapısı kırılmıştır)	TKIP/RC4 (WEP'in açıklarını kapatıyor)	CCMP/AES CCMP/TKIP
Şifreleme Anahtarı	40 bit	128 bit	128 bit
IV	24 bit	48 bit	48 bit
Anahtar Değişikliği	Anahtar sabittir	Anahtarlar her oturum, her paket için değişir	Anahtar değişikliğine gerek yoktur
Anahtar Yönetimi	Anahtar yönetimi yoktur	802.1x	802.1x
Asıllama	Zayıf bir yöntem	802.1x EAP	802.1x EAP
Veri Bütünlüğü	ICV	MIC	MIC