KABLOSUZ AĞ ŞİFRELEME YÖNTEMLERİNİN KARŞILAŞTIRILMASI

Coşkun Odabaş[1], İhsan Pehlivan[2], Serdar Demircioğlu[3], Mehmet Gezer[4], İlhan Coşkun[5]

[1, 2, 5] Sakarya Anadolu Teknik Lise, Teknik Lise ve End. Mes. Lis., Elekt.-Elektr. Tekn. Alanı, Sakarya, Türkiye

[3] Sakarya Üniversitesi, Mühendislik Fakültesi, Elektrik-Elektronik Mühendisliği Bölümü, Sakarya, Türkiye

[4] Sakarya Anadolu Teknik Lise, Teknik Lise ve End. Mes. Lis., Bilişim Tekn. Alanı, Sakarya, Türkiye

E-mails: [1]coskunodabas@hotmail.com, [2]ihsan333@yahoo.com, [3]serdar@deksanplywood.com, [4] mgezer@sakarya.edu.tr, [5]ilcoskun@hotmail.com

ABSTRACT

Amazing development of computer technologies and increasing of internet use are developing importance of wireless LAN. But, there is another important problem is exposed by this developing, "Security of Wireless LAN". Different encryption methods are used to solve this security problems. Some of these methods are WEP, WEP2, WPA, WPA2 and RADIUS. In this article, advantages and disadvantages of these encryption methods of wireless LAN are examined and discussed

Bilgisayar teknolojisinin ve özellikle internet kullanımının hızla artması kablosuz ağ teknolojisinin önemini gittikçe artırmaktadır. Ancak bu duruma paralel olarak ortaya çıkan çok önemli bir sorun kablosuz ağların güvenliğidir. Günümüzde bu sorunun çözülebilmesi için farklı şifreleme yöntemleri kullanılmaktadır. Bu yöntemlerden bazıları WEP, WEP2, WPA, WPA2 ve RADIUS'tur. Bu makalede kablosuz ağ şifrelemede kullanılan yöntemlerin birbirlerine göre avantajları ve dezavantajları incelenmiştir.

Key words: Wireless LAN, Encryption Methods, Wired Equivalent Privacy, Wi-Fi Protected Access, Wi-Fi Protected Access 2

1. GİRİŞ

Kablosuz teknolojisinin kullanımının hızla artmasının sonucu olarak tüm elektronik cihazların ve özellikle bilgisayarların birbirleri ile haberleştiği ağların kullanımı da artmış ve çok büyük önem kazanmıştır[1-3]. Kablosuz ağların kullanım alanların artmasına paralel olarak güvenlik sorunları da ortaya çıkmaya başlamıştır. Bu noktada en önemli iki sorun gerçekleştirilen haberleşmenin dinlenmesi ve yapılan veri transferlerinin istenmeyen kişiler tarafından ele geçirilmesi, diğer bir ifade ile bilgi hırsızlığıdır[2]. Kablosuz ağların güvenliğinin sağlanması için ağların şifrelenmesi yöntemi geliştirilmiştir. Bu amaçla yapılan ilk çalışma WEP şifrelemesidir.[4,10] WEP halen kullanılmakta olan bir uygulamadır ve yapılan ekleme ve düzenlemelerle güncelliğini korumaktadır. Ancak gönderilen veri paketlerinin yakalanmasının ve belirlenen şifrenin kırılmasının kolay olması nedeniyle güvenlik açısından en az tercih edilmesi gereken şifreleme yöntemidir. WEP'ten sonra ortaya atılan ve WEP'in dezavantajlarının bertaraf edilmeye çalışıldığı bir diğer şifreleme yöntemi ise WPA'dır. Format olarak WEP'e çok benzemekle birlikte belli noktaların değiştirilmesi ve şifreleme ile ilgili bazı eklentilerin yapılması ile birlikte daha güvenli bir şifreleme tekniği ortaya çıkartılmıştır. WPA2 son dönem şifreleme tekniği olarak dikkat çekmektedir. WPA'ya yeni algoritma teknikleri ve şifreleme verileri eklenerek ortaya çıkarılmıştır. Yüksek güvenlik ihtiyacı duyulan tüm uygulamalarda kullanılan WPA2 halen geliştirilmektedir[6-9].

Bu makalede ikinci bölümde kablosuz ağların güvenliği için kullanılan şifreleme yöntemleri ve bu şifreleme tekniklerinde kullanılan metotlar hakkında bilgi verilmiştir. Sonuçlar ve tartışma bölümünde ise kullanılan şifreleme yöntemlerinin karşılaştırması yapılarak avantaj ve dezavantajları değerlendirilmiştir.

2. KABLOSUZ AĞ ŞİFRELEME YÖNTEMLERİ

2.1. WEP (Wired Equivalent Privacy)

802.11 standardı, kablosuz alan ağlarında ortaya çıkan haberleşmelerin tanımlandığı bir standarttır. WEP (Wired Equivalent Privacy) algoritması her türlü harici saldırıdan kablosuz haberleşmeyi korumak için kullanılır. WEP'in ikinci fonksiyonu ise kablosuz ağa yetkisiz erişimleri engellemektir. WEP bir mobil cihaz istasyonu ve erişim noktası arasındaki kablosuz haberleşme kurmak ve paylaşımda bulunabilmek için bir şifreye ihtiyaç

duyar. Bu şifre ya da güvenlik anahtarı veri paketlerini göndermeden önce onları şifrelemek ve gönderim sonrasında değişikliğe uğrayıp uğramadıklarını için diğer bir ifadeyle doğruluk kontrolü yapmak amacıyla kullanılır. [10].

2.1.1. WEP'te Şifreleme

WEP'te kablosuz haberleşmenin güvenliğinin sağlanabilmesi için üç adım gerçekleştiril mektedir. Bunlar; kimlik doğrulama, gizlilik, bilgi değiştirme kontroludür

Bu denetimlerin haricinde güvenliğin artırılması için yapılması gereken Cevap Kontrolü (*Replay Control*), Erişim Kontrolü, Anahtar Dağıtımı ve Korunması gibi işlemlere ise WEP'te hiç yer verilmemiştir. WEP'te haberleşmenin ilk adım kimlik doğrulamadır. Bu adımda ağa bağlanan kişinin gerçekten ağa bağlanma yetkisinin olup olmadığının düzenlenmesi yapılır. Bundan sonraki ikinci adım ise ağa bağlı kişinin trafiğinin diğer kişiler tarafından izlenilememesinin sağlanmasıdır. WEP'te kimlik doğrulaması işlemi dört adımda gerçekleştirilir;

1. Bağlanma isteği ve AP rasgele bir metin oluşturur(128 bit) ve kablosuz cihaza gönderir.
2. Cihaz kendisindeki WEP şifresi ile gelen metni şifreler ve AP'ye şifrelenmiş metni gönderir.
3. AP geri gelen şifreleniş metnin doğruluğuna onay verir.

Gerçekleştirilen bağlantı tipi "Open Security" olsaydı cihaz Onay Mesajı (***Authentication Message***) istek gönderirken Algoritma Numarasını **0** olarak gönderecekti, bağlantı WEP ise bu numara **1** olur. İkinci adım ise güvenlik, diğer bir ifade ile şifreleme adımıdır. WEP şifreleme akışı olarak bilinen RC4 şifreleme algoritmasını kullanır. Akış şifreleyicisi, sonsuz değerde anahtar üreten bir sistemde gerektiği zamanlarda şifreleme anahtarı üreterek çalışır. RC4 şifreleme algoritması XORing yöntemini kullanmaktadır. Burada orijinal metin ile RC4 şifreleme anahtarı XOR'lanarak şifreli metin elde edilir.

Orijinal Metin (PlainText) **XOR** RC4Byteları = Şifreli Metin (Chipertext)

Gönderici cihazın şifreleme için kullandığı anahtarın aynısı alıcıda da bulunur. Alıcı bu anahtarı kullanarak kendi akış şifresini üretir. Daha sonra bu akış şifresi ile kendine gelen şifreli metni XOR işlemine tabii tutarak orijinal metni elde eder.

Şifreli Metin (ChiperText) **XOR** RC4Byteları = Orijinal Metin (PlainText)

Son adım olan Bilgi Değiştirme Kontrolünde ise gönderilen paket ya da mesajların ulaşım esnasında bir değişikliğe uğrayıp uğramadığının kontrolü yapılır. Bu kontrol için gönderilen paketler içerisine bir Integrity Check Vector alanı kullanılır. Ayrıca aynı akış anahtarı ile farklı metinlerin şifrelenmesini önlemek içinse her pakete paylaşılan bir gizlilik anahtarı ve farklı bir RC4 anahtarı eklenir. Ancak bu yöntemlerin olması gerektiği gibi kullanılmaması durumunda gizlilikte büyük açıklıklar meydana gelecek, gönderilen veri paketleri ve mesajlar değişikliğe uğrayacak ya da harici kullanıcılar tarafından elde edilip şifreleri çözülebilecektir. ICV alanı veri paketlerinin her biri için CRC32 sağlamsına benzer bir işlem gerçekleştirir.

WEP'te gönderilen şifreli metnin ya da verinin tekrar oluşmaması ve veri paketinin başlangıç durumunun belirlenmesi için IV – (Initialization Vector) vektörü kullanılır. Bu değer 64 bitlik WEP algoritması ile şifrelenmiş 64 bitlik veri paketlerinin 24 bitlik kısmını oluşturur ve iletişim trafiği ile birlikte sürekli artan bir değerdir. Bu sebeple WEP paketlerinin veri alanları 40 bittir. IV değeri paket içerisinde şifrelenmez; çünkü şifre çözme (*decrypt*) işlemi alıcı tarafında kullanılmaktadır. IV için ayrılan alanın küçüklüğü aynı akış şifresinin tekrar üretilmesi ihtimalinin yükselmesi anlamına gelir ve bu güvenlik için istenmeyen bir durumdur. 11Mbps'lik bir erişim hızında 1500 byte'lik paketler gönderen bir Access Point yaklaşık olarak $1500x8/(11x10^6)x2^{24}=18000$ saniyede bir ürettiği kış şifresini yinelemesi anlamına gelir. Bu durumda bir saldırganın aynı metne ait şifrelenmiş veri paketlerini ve bu paketlere ait IV bilgilerini toplayarak orijinal metni elde etme imkanı artmaktadır. IV'nin farklı bir kullanılma amacı da aynı metnin iki defa geçmesi durumunda farklı şifrelenmiş çıktıların oluşmasını sağlamaktır. Aksi takdirde yine kriptografik ataklar çok daha kolay olacaktır[4].

2.1.2 Standartlandırılmamış WEP Düzenlemeleri

Zamanla WEP'te görülen güvenlik açıkları ve iletişim problemlerini gidermek için WEP şifreleme algortimasında bazı değişiklikler yapılmıştır. Bu düzenlemeler aşağıdaki gibidir;

1. WEP2; bu değişiklikle başlangıç değeri olan IV 24 bitten 128 bite yükseltilmiştir. Bu sayede üretilen IV değeri miktarı artırılarak veri paketlerinin istenmeyen alıcılar tarafından yakalanması durumunda dahi orijinal metnin elde edilmesi ihtimali düşürülmüştür.

2. WEP+; şifrelemede kullanılan, çözülmesi ve yakalanması kolay olan IV vektörlerinin kullanımdan çıkartılması esasına dayanır.
3. Dynamic WEP; bu düzenleme WEP anahtarlarının dinamik ve sürekli olarak değiştirilmesi esasına dayanır[4].

2.2 WPA (WI-FI PROTECTED ACCESS)

Orijinal 802.11 standardı kablosuz ağların güvenliği konusunda şu güvenlik özelliklerini sağlar; iki ayrı kimlik denetim metodu; açık sistem ve paylaşılan anahtar, WEP şifreleme algoritması ,WEP şifrelemede veri bütünlüğünün sağlanabilmesi için bir Bütünlük Kontrol Değeri (Integrity Check Value (ICV)).

Ancak yukarıda belirtilen güvenlik özellikleri özellikle çok büyük ağlarda ya da yüksek veri trafiğinde yetersiz kalmaktadır. 802.11 standardı güvenlik açısından şu sorunları içerir;

1. Her kullanıcı için kimlik denetimi ve kontrol yoktur.
2. Harici kimlik denetim uygulamalarını desteklemez.
3. Her oturum ya da her istemci için dinamik anahtar yönetimini desteklemez.

Yukarıda belirtilen sorunların tamamı 802.1X Port Bazlı Ağ Erişim Kontrolü (Port-Based Network Access Control) standardı ile çözülmüştür. IEEE 802.11i standardı, 802.11 için söz konusu olan birçok gizlilik ve adresleme sorunlarının çözüldüğü yeni geliştirilmiş bir kablosuz ağ standardıdır. IEEE 802.11i standardının yeni bir kablosuz ağ standardı olarak kabul edilmesi ile birlikte yeni bir güvenlik standardı da ortaya atılmıştır. Bu standart Wi-Fi Protected Access (WPA)'dır. WPA standardı aşağıdaki hedefleri gerçekleştirmektedir;

1. Kablosuz ağların için güvenlik oluşturmak.
2. bir yazılım güncellemesi boyunca oluşabilecek sorunların kaydetmek.
3. Ev ve küçük ofis (SOHO) kullanıcıları için kablosuz ağ güvenliğini sağlamak[9].

2.2.1 WPA Güvenliğinin Özellikleri:

WPA aşağıdaki gizlilik özelliklerini sağlar.

2.2.1.1 WPA kimlik denetimi:

802.1X kimlik denetimi 802.11 ile opsiyonel hale getirilmiştir. Ancak WPA ile kimlik denetimi zorunlu olmuştur. Kimlik denetimi aşağıdaki belirtilen iki aşamada oluşturulur.

1. İlk aşama açık sistem kimlik denetiminin kullanılması ve kablosuz istemcinin veri paketi göndermek için kablosuz erişim noktasına sinyal göndermesidir.
2. İkinci aşama ise 802.1X standardının kullanıcı seviye kimlik denetimini gerçekleştirmesidir.

WPA, RADIUS altyapısına sahip olmayan çevre cihazları için sadece ön paylaşım anahtarını destekler. RADIUS altyapısına sahip cihazlar içinse hem RADIUS hem de EAP destği söz konusudur[9].

2.2.1.2 WPA Key yönetimi:

WPA şifreleme yönteminde unicast ve global şifreleme anahtarları için rekeying işlemi zorunludur. Geçici Bütünlük Anahtar Protokolü/Temporal Key Integrity Protocol (TKIP) her bir veri çerçevesi için kullanılan şifreleme anahtarını sürekli olarak değiştirir ve her bir değişimde kablosuz erişim noktası ve kablosuz istemcilerin senkronizasyonunu sağlar[9].

2.2.1.3 Temporal key integrity protocol (TKIP)

WEP şifreleme özelliği 802.11 standardı için opsiyoneldir. WPA içinse, TKIP kullanımı zorunludur. TKIP; şifreleme anahtarlarının belirlenmesinden sonra gizlilik konfigürasyon larının doğrulanmasında ve ver bir unicast veri çerçevesinin şifreleme anahtarlarının değişimde donanımlar arası. senkronizasyonun sağlanma sında kullanılır[9].

2.2.1.4 Michael

WPA ile Michael olarak bilinen ve 8 byte'lık Message Integrity Code (MIC) bilgisinin kullanıldığı yeni bir algoritma kullanılmaya başlanmıştır. MIC bilgisi 802.11 veri çerçevesinin veri alanı ile 4 byte'lık ICV bilgisi arasına yerleştirilir. MIC alanı, veri ve ICV ile birlikte şifrelenir. Michael algoritması WPA için ayrıca ekstra güvenlik sağlar[9].

2.2.2 WPA Geçici Anahtarları

WEP'ten farklı olarak, WPA şifreleme yönteminde unicast veri şifrelemesi için tek bir anahtar, mulicast ve broadcast veri için ise tip olarak farklı bir key kullanılır. Bunun yanı sıra her bir Erişim noktaı ve istemci çifti için dört farklı key ve son olarak multicast ve broadcast trafiği içinse iki farklı key kullanılır. LAN içerisinde ve EAP ve unicast data içinse bir anahtar çifti kullanılır. Anahtar mesajları aşağıdaki bileşenleri içerir;

a. Veri Şifreleme Anahtarı (Data Encrytion Key): Unicast veri çerçevelerinin şifrelenmesi için kullanılan 128 bitlik anahtar.
b. Veri Bütünlük Anahtarı (Data Integrity Key): Unicast veri çerçeveleri için MIC hesaplanmasında kullanılan 128 bitlik anahtar.
c. EAPOL-Key Şifreleme Anahtarı (EAPOL-Key encryption key): EAPOL-Key mesajlarının şifrelenmesi için kullanılan 128 bitlik anahtar.
d. EAPOL-Key Bütünlük Anahtarı (EAPOL-Key integrity key): EAPOL-Key mesajları için MIC hesaplanmasında kullanılan 128 bitlik anahtar.

Yukarıda belirtilen EAPOL-Key bilgileri her bir cihaz için (Erişim noktası ve istemci) MAC adreslerini ve cihazlarda rasgele üretilen sayıları içerir. Ayrıca duruma göre MIC bilgileri de bulunabilir[9].

2.2.3 WPA Şifreleme ve Şifre Çözme İşlemleri

WPA, kablosuz veri çerçevesini şifrelemek ve bütünlüğünü korumak için aşağıdaki değerlere ihtiyaç duyar;

1. Sıfırdan başlayan ve her dizi çerçevesi için sürekli artan IV değeri.
2. Veri şifreleme anahtarı ya da grup şifreleme anahtarı.
3. Kablosuz veri çerçevesinin kaynak (SA) ve hedef (DA) adresi.
4. Sıfırdan başlayarak artan ve gelecek işlemin belirtilmesi için ayrılan özellik alanının değeri.
5. Veri ya da grup bütünlük anahtarı[6].

Aşağıda bir unicast veri çerçevesi için gerçekleştirilen WPA şifrelemesinde uygulanması gereken aşamalar belirtilmekledir;

1. IV, DA ve veri şifreleme anahtarı bir WPA anahtar karıştırma fonksiyonuna girilerek her paket için şifreleme anahtarı hesaplanır.
2. DA, SA, öncelik alanı, veri, veri bütünlük anahtarı Michael veri bütünlük algoritmasına girilerek MIC elde edilir.
3. CRC-32 sağlaması ile ICV değeri hesaplanır.
4. IV ile şifreli her paket RC4 PRNG fonksiyonuna girilerek, MIC ve ICV ile aynı veri genişliğindeki bir akış anahtarı üretilir.
5. Veri, MIC ve ICV kombinasyonu ile akış anahtarı XOR işlemine tabii tutularak şifrelenmiş metin elde edilir.
6. Şifrelenmiş metne IV ve genişletilmiş IV bilgileri eklenerek tüm dizileri içeren bir 802.11 kablosuz veri çerçevesi elde edilmiş olur[6].

Bir unicast veri çerçevesi için gerçekleştirilen şifre çözme işlemi aşamaları aşağıda belirtildiği gibidir;

1. IV değeri 802.11 çerçevesindeki şifreli metin ile genişletilmiş IV değerinden çıkartılarak, DA ve veri şifreleme anahtarı ile birlikte anahtar karıştırma fonksiyonuna girilir. Bu işlem sonucunda her paket için şifreleme anahtarı üretilir.
2. IV ve her paketin şifreleme anahtarı RC4 PRNG fonksiyonuna girilerek MIC, ICV ve şifreli metin ile aynı boyuta sahip bir akış anahtarı üretilir.
3. Akış anahtarı şifreli veri, MIC ve ICV ile XOR'lanır. Bu işlem sonucunda şifresiz metin, MIC ve ICV üretilir.
4. ICV ile şifresiz ICV karşılaştırılır. Eğer değerler birbirini tutmazsa veri kabul edilmez.
5. DA, SA ve veri bütünlük anahtarı Michael bütünlük algoritmasına girilerek MIC değeri üretilir.
6. Hesaplanan MIC değeri ile şifresiz MIC değeri karşılaştırılır. Eğer MIC değerleri eşleşmez ise veri kabul edilmez. MIC değerleri eşleşirse veri işlenmesi için üst katmanlara gönderilir[6].

2.3 WPA 2 (WI-FI PROTECTED ACCESS 2)

WPA 2 şifrelemesi hem teorik hemde pratik açıdan çoğu noktada WPA ile benzer bir şifreleme teknolojisidir. WPA şifrelemesi ile birlikte kullanılmaya başlanan kimlik tanımlama, anahtar yönetimi gelişmiş şifrleme standartları (AES) gibi uygulamalar WPA 2 için de geçeridir.
Bu özelliklerin yanı sıra WPA 2'de ekstra özellikler de mevcuttur. Bunlar arasında veri alışverişi yapılmadan önce yapılan ön kimlik denetimi, daha önce bağlantı kurulan erişim noktasının kimlik bilgilerinin tutulduğu PMK önbellekleme sayılabilir. Bu özellikler ayrıca şifreli haberleşmenin hızlanmasını sağlamaktadır.[7]

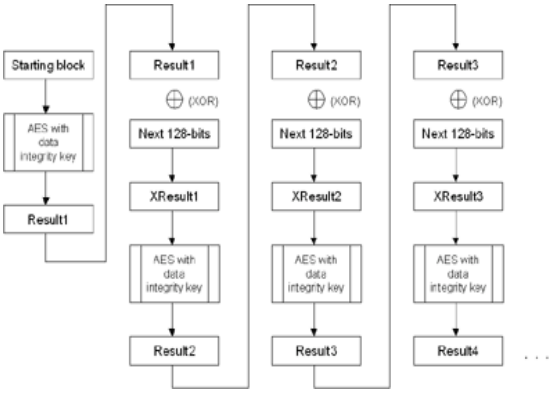
2.3.1 WPA 2 Şifreleme ve Şifre Çözme İşlemleri

WPA 2'nin kriptografik özellikler ve şifrelemede kullandığı geçici anahtarlar bütünüyle WPA'dakinin aynısıdır. WPA 2'de MIC değerinin üretilmesi için CBC-MAC algoritması kullanılır. MIC değerinin hesaplanmasında CBC-MAC algoritması aşağıdaki işlemleri yapar;

1. AES ve veri bütünlük anahtarı 128 bitlik bir başlama bloğu ile şifrelenir. Bu işlem sonucunda 128 bitlik Result1 değeri elde edilir.
2. Result1 değeri ile verinin bir sonraki 128 bitlik değeri XOR işlemine tabii tutularak MIC değeri bulunur. Bu değer aynı zamanda XResut1 değeridir.
3. XResult1 değeri ile AES ve veri bütünlük değeri şifrelenir bu işlemin sonucunda Result2 değeri bulunur.

4. Result2 ile verinin sonraki 128 bitlik değeri XOR işlemine tabii tutulur. Bunun sonucunda XResult2 değeri bulunur.

3. ve 4. adımlar verinin tamamına 128 bitlik bloklar halinde uygulanır. Bu şekilde verinin tamamı şifrelenmiş olur. WPA 2'de şifre çözme işlemi gerçekleştirilen işlemlerin tam tersinin yapılması ile oluşturulur[8].



Şekil 1: WPA 2'de şifreleme işlemi

3. SONUÇLAR VE TARTIŞMA

Kablosuz haberleşmelerin güvenliği için şifreleme vazgeçilmez bir hale gelmiştir. Bu alanda yapılan uygulamalar avantajları ve dezavantajları ile kullanıcıların hizmetine sunulmuştur. Şifreleme yöntemleri içerisinde en zayıf ve güvenilirliği en düşük olan yöntem WEP şifrelemesidir. Günümüzde WEP şifrelemeleri her türlü saldırıya açık durumdadır. Bunun sebebi olarak WEP'te IV değerinin çok düşük olması, veri bütünlüğünün zayıf olması, rekeying korumasının olmaması, tekrar koruma işleminin yapılmaması sayılabilir. Bu dezavantajlar WEP'te yapılan bazı düzenlemeler ve sürümler ile giderilmeye çalışılmışsa da tam anlamıyla güvenlik sağlanamamıştır.

WEP'ten daha sonra ortaya çıkarılan WPA ve WPA2 şifreleme yöntemleri ile güvenlik daha da artırılmış ve gönderilen verilerin bütünlüğü korunmuştur. Bu amaçla WEP'te 24 bit olan IV değeri 48 bite çıkarılmış, Mikael ve CBC-MAC gibi algoritmalar ile ekstra şifreleme işlemleri yapılmış, ayrıca güvenlik seviyesinin artırılması için değişik özelliklerde ve çok sayıda şifreleme anahtarı kullanılmıştır. Tüm bu incelemelerin ışığında kablosuz ağ için en güvenilir şifreleme metodu olarak WPA 2 görülmektedir. Ancak WPA2 için çok önemli bir dezavantaj söz konusudur ki bu da şu an için WPA 2 uyumlu donanım cihazlarının yeteri kadar bulunmaması ve mevcut olan cihazların maliyetinin yüksek olmasıdır. Bununla birlikte WPA 2 uyumlu cihazların WEP ve WPA ile de uyumlu olduğu söylenebilir.

KAYNAKLAR:

[1] Jyh-Cheng Chen, Ming-Chia Jiang, Yi-Wen Liu, (2005), "Wireless LAN Security and IEEE 802.11i", *IEEE Wireless Communications,* 12(1), 27-36

[2] L. Hu and D. Evans,(2003)" Secure Aggregation for Wireless Networks," Proc. Symposium on Applications and the Internet Workshops, pp.384-391,

[3] Wong Stanley, (2003), "The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards", GSEC Practical v1.4b, 1-10.

[4] Borisov Nikita, Goldberg Ian, Wagner David, (2001), "Intercepting mobile communications the insecurity of 802.11", *Proceedings of the 7th annual international conference on Mobile computing and networking*, *Italy,* 180-189

[5] Improving Security in Wireless Networks, www.3com.com, Open Servis Networking,

[6] Microsoft TechNet, Networking and Access Technologies, Wi-Fi Protected Access Data Encryption and Integrity, http://technet.microsoft.com/en-us/library/bb878126.aspx

[7] Microsoft TechNet, Networking and Access Technologies, Wi-Fi Protected Access 2 Overview, http://technet.microsoft.com/en-us/library/bb878054.aspx

[8] Microsoft TechNet, Networking and Access Technologies, Wi-Fi Protected Access 2 Data Encryption and Integrity, http://technet. microsoft.com/en- us/library/bb878096.aspx

[9] Microsoft TechNet, Networking and Access Technologies, Wi-Fi Protected Access Overview, http://technet.microsoft.com/en-us/library/bb877996.aspx

[10] Stubblefield Adam, Ionnidis John, Rubin Aviel, (2002), "A Key Recovery Attack on The 802.11b Wired Equivalent Privacy Protocol (WEP)", 1-15