T.C.
İSTANBUL TEKNİK ÜNİVERSİTESİ
Bilişim Enstitüsü

AĞ GÜVENLİĞİ

Prof. Dr. Bülent ÖRENCİK

"WiMAX Güvenliği"

Dönem Raporu
13-04-2007

Yük. Müh. Berk CANBERK
704042007

DİZİN

1. GİRİŞ
    a. IEEE 802.16 Standardı ve WiMAX Forumu
    b. IEEE 802.16'nın Genel Yapısı
        i. İletişim Temelleri
        ii. Katmansal İnceleme

2. IEEE 802.16 GÜVENLİK ALTYAPISI
    a. Standardın Genel Yapısı
    b. Güvenlik Birimi'nin İncelenmesi
    c. Veri Güvenliği Düzeyi
    d. Güvenlik Yönetimi Düzeyi
    e. 802.16 Örgü (Mesh) Yapılarda Güvenlik Unsurları

3. 802.16 GÜVENLİK ALTYAPISININ ANALİZİ
    a. Veri Şifrelemesindeki Sorunlar
    b. Anahtar Yönetimindeki Sorunlar
    c. Asıllamadaki Sorunlar

4. SONUÇ

5. YARARLANILAN KAYNAKLAR

KISALTMALAR

WiMAX: Worldwide Interoperability for Microwave Access
SS: Subscriber Station
BS: Base Station
LOS: Line of Sight
NLOS: Non-Line of Sight
PMP: Point to Multipoint
QAM: Quadrature Amplitude Modulation
OFDM: Orthogonal Frequency Division Multiplexing
PKM: Privacy Key Management
SA: Security Association
SAID: Security Association Identifier
CID: Connection Idendifier
CBC: Cipher Block Chaining
DES: Data Encyrption Standard
RSA: Rivest-Shamir-Adlemon Public Key Algorithm
AES: Advanced Encyrption Standard
AK: Authentication Key
TEK: Traffic Encyrption Key
KEK: Key Encyrption Key
HMAC: Hashed Message Authentication Code
EAP:Extensible Authentication Protocol

ŞEKİLLER

Şekil-1: Tek noktadan çok noktaya (PMP) 802.16 ağ yapısı
Şekil-2: Örgü (Mesh) 802.16 ağ yapısı
Şekil-3: 802.16 2.katmanındaki güvenlik altkatmanı
Şekil-4: Şifreleme bloklarını aradarda bağlama kipinde (CBC) çalışan DES
Şekil-5: Asıllama anahtarı (AK) istek-cevap diyagramı
Şekil-6: TEK istek-cevap diyagramı
Şekil-7: Merkezi örgü (Centralized Mesh) 802.16 ağ yapısı

1. GİRİŞ

a. IEEE 802.16 Standardı ve WiMAX Forumu

1990'lı yıllarda artan teknolojik gelişimler, sayısal haberleşmeye karşı duyulan hevesle birleşince telsiz iletişime olan eğilimde artmıştır. IEEE, telsiz iletişim standardı olarak ortaya çıkarttığı 802.11 WLAN'den sonra benzer bir yapıyı kentsel alan ağları için geliştirmeye başlamıştır. Bu amaçla IEEE, 1999 yılında, geniş bantlı telsiz kentsel alan ağı (Wireless Metropolitan Area Network, Wireless-MAN) standardının ilk adımlarını atmaya başlamıştır. 2001 yılında tam olarak şekillenen bu standard 2005 yılına kadar gelişmesini tamamlamıştır.

Buna paralel olarak 2001 yılında, başını INTEL'in çektiği bir oluşumuna gidilmiş ve telsiz haberleşme konusunda altyapı deneyimleri dünyaca onanmış INTEL, ALVARION, FUJITSU ve SAMSUNG firmalarının önderliğinde bir forum kurulmuştur. WiMAX (Worldwide Interoperability for Microwave Access) adını alan bu forum IEEE 802.16 standartlarını temel alan ürünler geliştirmekte ve bu konuda çalışmalar yapmaktadır. Günümüzde 400'e yakın kurumsal üyesi olan bu forum kentsel ağlarda geniş bantlı telsiz iletişim altyapısının oluşumunda faaliyetlerine devam etmektedirler.

b. IEEE 802.16'nın Genel Yapısı

IEEE 802.16 standardını iki alt başlıkta incelemek mümkündür:

i. Iletişim temelleri

2001 yılında oluşturulan 802.16a standardında, frekans aralığı 10-66 GHz olarak tasarlanmıştır.Bu yüksek frekans "görüş alanında bulunan (Line Of Side-LOS)" cihazlardan kurulu bir ağ için düşülmüştür. Erişilebilecek maximum hız 34 Mbps olup kapsama alanı 5 km'ye kadardır. 2004 yılında son halini alan 802.16 (802.16d) ile sadece "doğrudan görüş alanı" için değil "görüş alanı içinde olmayan (Non-LOS)" yapılar da hedeflenmiştir. Frekans bandı 2-11 GHz olarak tasarlanmış ve maximum hız 70Mbps'a kadar çıkmıştır. Teorik kapsama alanı 70 km olarak belirtilmiştir.

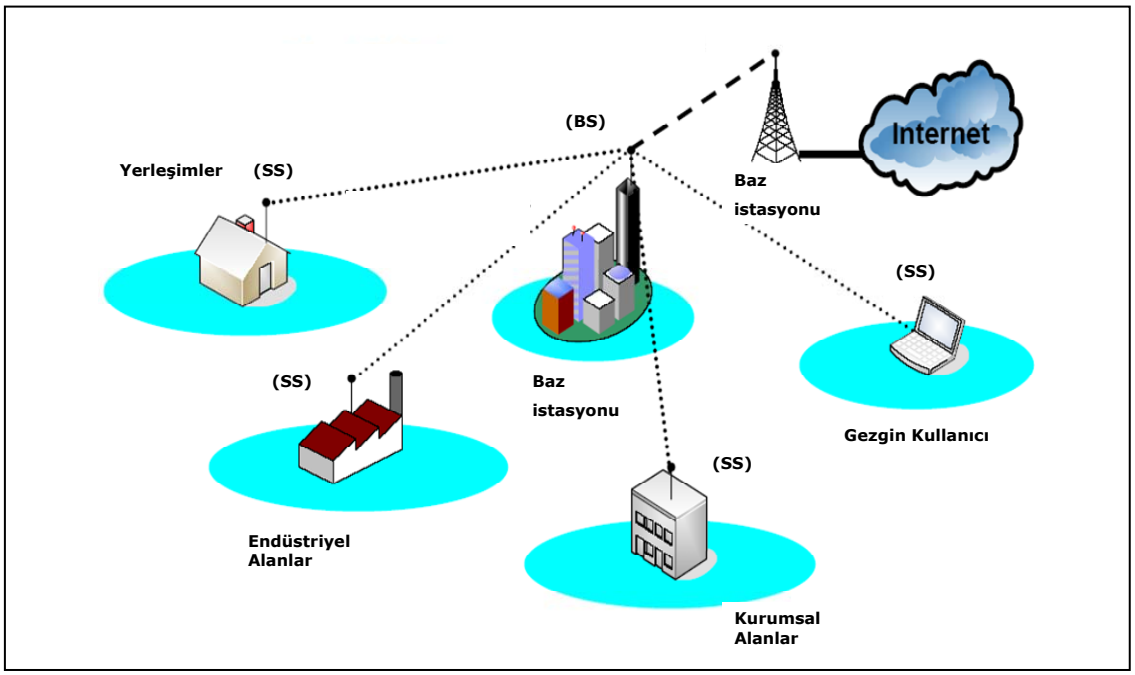
802.16 iletişim yapısı

- Tek noktadan çok noktaya(Point-to-Multipoint-PMP)
- Örgülü (MESH)

olarak ikiye ayrılır.

Tek noktadan çok noktaya iletişim:
Uç birimler yada başka bir değişle kullanıcı istasyonları(Subscriber Stations-SS) bir baz istasyonu (BS) ile iletişim halindedirler. Tüm haberleşme parametreleri BS tarafından kontrol edilir. Bu durumda SS'den BS'e doğru akan trafiğe "uplink", BS'den SS'e doğru akan trafiğe ise "downlink" denir. bu iki trafikte aynı

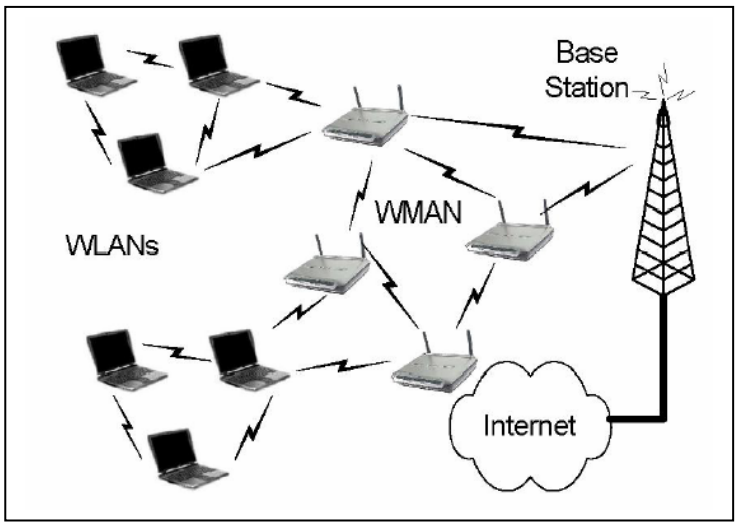
çerceve üzerinden çeşitli parametler yardımıyla BS tarafındn control edilir (Downlink Map ve Uplink Map alanları çercevede bu amaç için kullanılan alanlardır). Bu tarz bir yapı şekil-1'de görülmektedir.



Şekil-1
Tek noktadan çok noktaya (PMP) 802.16 ağ yapısı

Örgü tipi iletişim:

SS'ler BS ile doğrudan bir bağlantı içine girmezler. SS'ler kendi içlerinde de birbirleriyle bağlantı kurabilir ve bu bağlantıyı yönetebilirler. Burada tek-katmanlı[1] bir yapıdan (single-hop) çok, çok-katmanlı[2] (multi-hop) bir yapı söz konusudur. Örgü yapısında BS iletişimi kontrol eden bir şekilde de bulunabilir, ki bu yapı merkez-örgü şeklinde adlandırılır (Centralized Mesh), ya da SS'ler BS'in gözetimi altında olmadan haberleşmeyi yapabilirler (Distributed Mesh). Bu tarz bir yapı şekil-2 de görülmektedir.



Şekil-2
Örgü (Mesh) 802.16 ağ yapısı

[1] Single-hop: SS ile BS doğrudan bağlıdırlar.Tek bir zıplama ile SS BS'e ulaşır.
[2] Multi-hop: SS,BS'e tek zıplamada ulaşamaz.Söz konusu SS, BS ile başka SS'leri geçerek iletişime geçebilir.

ii. Katmansal İnceleme

802.16'nın yapısal farklılığı birinci ve ikinci katmanda karşımıza çıkar. Kapsama alanındaki genişleme ve hızdaki artış, bu teknolojide yeni modulasyon teknikleri kullanılmasını gerektirmiştir. 64-QAM[3] modulasyon tekniği, 802.16d standardında kullanılır.

Ikinci katmandaki çoklama OFDM temellidir. 802.16 standardının en temel özelliklerinden biri, ikinci katman MAC'ının yarış tabanlı (contention-based) değil planlı ve bağlantılı bir yapıda (scheduled, connection oriented-MAC) olmasıdır. Böyle bir yapı olması ile, BS iletişime başladığı tüm SS'lerle kesintisiz ve kaliteli bir alışveriş sağlar. Işte bu kalite arttırımı 802.16 standardının sadece saf veri gönderiminde değil, kaliteli ve gecikmeye hassas veri gönderiminde de kullanımımın çok elverişli olmasını sağlamıştır.

802.16 temelli WiMAX altyapısı temel olarak şu tür iletişimler için elverişlilik ve etkinlik getirmiştir:

- Saf veri: e-posta ve dosya alışverişi
- Isteğe bağlı gerçek zaman verisi
  - Isteğe bağlı ses
  - Isteğe bağlı video
- Videokonferans
- VoIP (voice over IP)

2. 802.16 GÜVENLİK ALTYAPISI

a. Standardın Genel Yapısı

802.16, sağladığı yüksek band genişlikli telsiz iletişiminin doğası gereği birçok güvenlik tehdidi ile karşı karşıya bulunmaktadır. Bundan dolayı ikinci katmanda özel bir "güvenlik altkatmanı" oluşturulmuştur. Bu katman bağlantıdaki tüm güvenlik unsurlarıyla ilgilenir.

Güvenlik katmanı iki düzeye ayrılmaktadır:

1. Veri güvenliği düzeyi

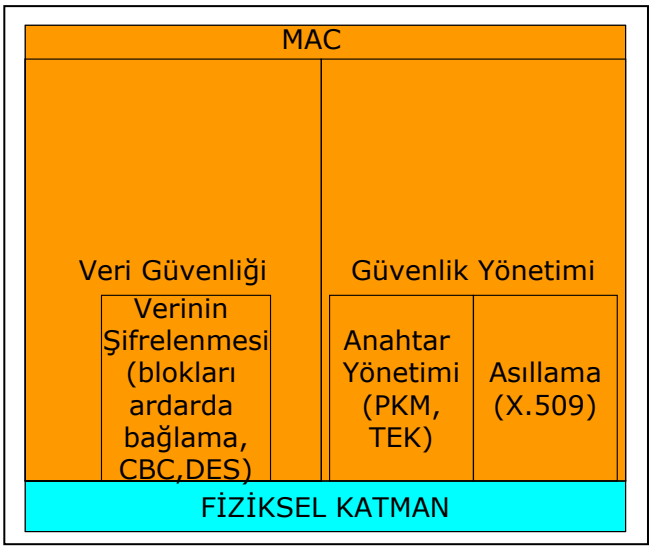
Gönderilecek verinin şifrelenmesinde kullanılacak algoritma, bu algoritmanın sorunsuz çalışması için gerekli parametler ve şifreleme kiplerinin bilgilerinin tutulduğu düzeydir.

2. Güvenlik Yönetimi düzeyi

Hem anahtar yönetimi hem de asıllamanın yapıldığı düzeydir. Oturum anahtarlarının değiştokuşu, şifreleme algoritmaların kullacağı anahtarların oluşumu, asıllama için gerekli sertifikaların alınması,bunların bağlantı sırasında BS'e gönderilmesi bu düzeyin görevleri arasındadır.

[3] 64-QAM: 64 sembolün module edildiği ve faz açılarına dayalı bir modulasyın tekniğidir.

Bu iki düzey şekil-3'te gösterilmiştir.



Şekil-3
802.16 2.katmanındaki güvenlik altkatmanı

İki düzeyin kontrol edildiği güvenlik altkatmanı, bu kontrolü 5 değişik kavrama dayalı bir yapıyla sağlar. Bu kavramlar:

- Veri Şifreleme

MAC çerçevesindeki veri kısmına uygulanır. Başlık kısmına uygulanmaz. Veri şifrelenmesinde başlık kısmının açık olarak gönderilmesi, hem SS'le BS arasındaki bağlantının basitliği hem de taraflardaki MAC yapılarının normal işleyişini devam ettirmeleri açısından tercih edilmiştir. Eğer şifrelenmiş olarak gönderilseydi hangi SS'in bağlantı kurmaya çalıştığı anlaşılmayacak buda sistemin düzgün çalışmamasına sebep olacaktı.

- Anahtar Yönetimi

SS, kendisini BS'e tanıtmak, bağlantı sırasında kullacağı anahtarı elde etmek için "Privacy Key Management-PKM" kullanır. X.509 sertifikalandırması ile SS kendisini BS'e tanıtır. PKM, güvenlik altkatmanı tarafından hem asıllamada hem de anahtar alışverişinde kullanılır. PKM, bir açık anahtar yapısı kullanarak oturum anahtarını elde eder. Bu oturum anahtarı, hem BS ve SS arasındaki oturumun kurulması(asıllama) ve devamını hem de oturumdaki veri alışverişinin güvenliği için yapılması gereken şifrelemede kullanılacak anahtarın üretilmesini(anahtar değişimi) sağlayacak bir anahtardır. Bunun yanında, tüm SS'ler bir açık anahtar-gizli anahtar çifti ile donatılmıştır. Bu yapı genelde RSA algoritması ile sağlanır.

- "Güvenlik Birimi" 'nin oluşturulması

802.16 ağlarında, SS ve BS arasında oluşması planlanan güvenlik ortamının yaratılması, güvenli veri iletişiminin yapılması ve bağlantının güvenli bir şekilde sonlandırılmasını sağlayan yapı "güvenlik birimi (Security Association-SA) olarak adlandırılmıştır. Üç tip güvenlik birimi kurulabilir:

- Birincil Güvenlik Birimi (Primary SA): Bağlantı kurulduğunda yaratılır.

- Statik Güvenlik Birimi (Static SA): BS'te bağlantı sonrası oluşan SA'dır.
- Dinaik Güvenlik Birimi (Dynamic SA): Servis kalitesi ve istemine göre oluşup bozulabilen SA'dır.

Tüm SS ve BS'lerde bulunan güvenlik birimleri, 16-bitlik bir SAID(Security Assosication ID) belirteci ile kimliklendirilirler. Ayrıca üst katmandaki servis bağlantıları da güvenlik birimleri ile birer bağlantı belirteci (CID) ile eşleştirilir.

- Bağlantının güvenlik birimine iletilmesi

Bağlantının güvenlik birimiyle ilişkilendirilmesi güvenlik altkatmanının sorumluluğundadır. Burada tüm 4.katman bağlantıları birincil SA'larla eşleştirilmelidir. Ayrıca Multicast bağlantılar statik yada dinamik SA'larla eşleşmelidir.

- Kriptografik süreç

Bağlantının güvenli bir şekilde oluşması,asıllamaların gerçekleştirilmesi ve verinin şifrelenip gönderilmesi sırasındaki tüm kriptografik süreç (kullanılan metodlar,algoritmaların girdiği durumlar vs.) güvenlik altkatmanı tarafından denetlenir.

b. Güvenlik Biriminin incelenmesi

SS ile BS arasındaki bağlantının güvenliği için gerekli olan asıllama,anahtar değişimi ve verinin şifrelenmesi/şifresinin çözülmesi işlemlerinin gerçekleşmesini sağlayan bir yapıdır. Bu yapı üst katmandaki servislere saydamdır. SS'teki bir üst katman servis, güvenlik biriminin hangi düzeyinden ne şekilde bir bağlantı aracalığıyla BS'le haberleşeceğini bilmez,sadece belirlenen şifreleme ve asıllama protokolleriniden haberdardır. Diğer tüm işlemler güvenlik birimi tarafından saydam olarak gerçekleştirilir. Her güvenlik biriminin kendine özgü 16-bitlik bir belirteci (SAID) vardır. Üst katman bağlantılarının kimliklendirildiği bir belirtec (CID) SA tarafından verilir. Şifrelemede kullanılacak algoritma, başlangıç vektörü,anahtarlar ve bağlantı ID'leri güvenlik birimi tarafından yönetilir. Şekil-3'te gösterilen yapıdaki düzeylerin kontrolü güvenlik birimi tarafından gerçekleştirilir.

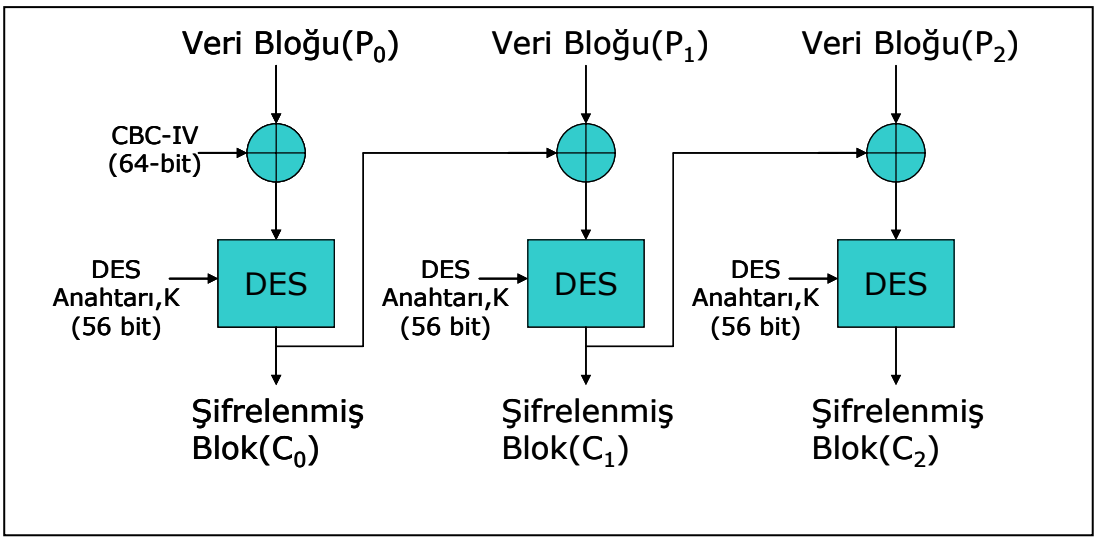
c. Veri Güvenliği Düzeyi

802.16 standardında kullanılan veri şifreleme algoritması, bir simektrik anahtarlı şifreleme algoritması olan DES'tir. 64-bitlik bloklar 56-bitlik anahtar yardımıyla şifrelenir. Kullanılan şifreleme kipi "şifreleme bloklarını aradarda bağlama kipi, (Cipher Block Chaining-CBC)" dir. Bu kip, kendisinden bir önce gelen şifrelenmiş bloğu, şifrelenmek üzere bekleyen blokla XOR'ladıktan sonra DES şifrelemesine gönderir. DES şifreleme algoritması kullandığı bir K anahtarı yardımıyla şifreli bloğu oluşturur. Benzer şekilde şifrelenmiş metin kendisinden önce gelen şifreli metin ve DES anahtarı ile çözülmüş o anki şifreli metinin XORlanması ile düz metin (P_i) haline getirilir. Bahsedilen şifreleme işlemi denklem-1 ile şifre çözme işlemi ise denklem-2 ile matematiksel olarak gösterilmiştir.

$$C_i = K\left[P_i \oplus C_{i-i}\right] \qquad \text{denklem-1}$$

$$P_i = C_{i-1} \oplus K^{-1}[C_i] \qquad \text{denklem-2}$$

Bir başlangıç vektörü(Initialization Vektor-IV) birinci bloğun şifrelenmesi için kullanılır. Başlangıç vektörünün değeri veri şifrelemesinde kullanılacak olan anahtarın değiştokuşu sırasında öğrenilirken, yapılacak olan işlem(yani XOR işlemi) başlangıçtaki senkronizasyon çerçeveleri tarafından öğrenilir. Şekil-4 bahsedilen CBC-DES'i göstermektedir



Şekil-4
Şifreleme bloklarını aradarda bağlama kipinde (CBC) çalışan DES

d. Güvenlik Yönetimi Düzeyi

Güvenlik yönetimi düzeyi iki bölümden oluşmaktadır. Bunlar asıllama ve anahtar değişimidir.

i. Asıllama

802.16'da asıllama için bir açık anahtarlı kriptografi kullanılmaktadır. SS ile BS tarafında bulunan SA'lar arasında bir SAID alışverişi de bu sırada gerçekleşir. Kendisini BS'e tanıtmak isteyen bir SS, X.509 sertifikalamasını kullanarak elde ettiği sertifikasını,dolasıyla açık anahtarını BS'e gönderir. BS, eğer kendisine gelen sertifikayı doğrularsa buna cevap vererek SS'i asıllar.

Burada kullanılan sertifikalar iki tip olarak yaratılır. Bunlardan birincisi üretici sertifikası diğeri ise SS sertifikasıdır. Üretici sertifikası, söz konusu SS cihazlarının üreticilerinden olan ve WiMAX forumuna üye tarafından oluşturulan bir sertifikadır. Kendi kendine bir yerel algoritma yada üçüncü bir şahıs tarafından verilebilen bu sertifikada üretici bilgileri yer almaktadır. Üretici sertifikasının yaratılmasındaki amaç WiMAX standardına uygun ürünlerin sisteme giriş yapmasını kontrol etmektir. Kullanılan

ikinci tip sertifika SS sertifikasıdır. Bu sertifika üretici tarafından meydana getirilir. SS'in seri numarası ve MAC adresini içeren bu sertifika ile SS kendisini BS'e tanıtır. Ayrıca SS'ler RSA tabanlı bir açık-gizli anahtar çifti ile donatılmıştır. Bu anahtarlarda SS'lerde yürütülen yerel algoritmalar yardımıyla yaratılıtırlar.

Asıllamanın aşamaları şu şekildedir:

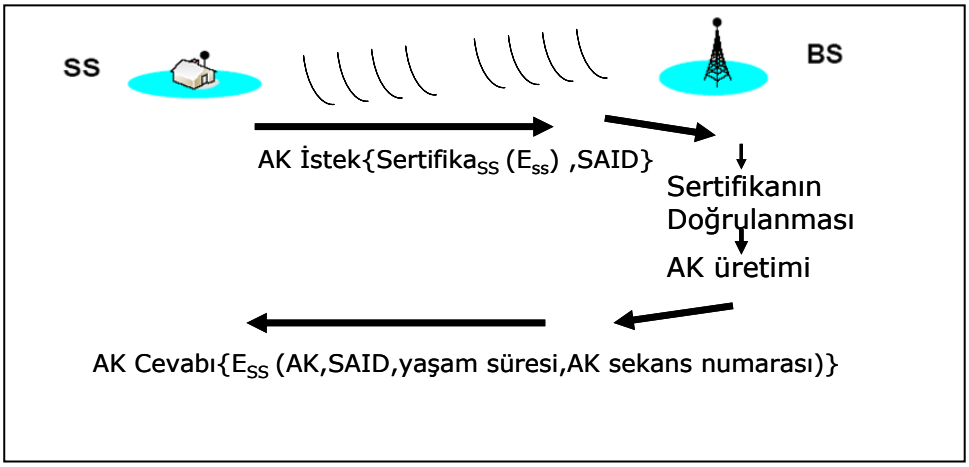
Birinci aşama: SS, BS'e üretici sertifikasını gönderir. Bu şekilde BS, WiMAX'e uygun bir üretici tarafından üretilen bir kullanıcıyla karşı karşıya olduğunu anlar.

İkinci aşama: SS, BS'e kendi sertifikasını (SS sertifikası), güvenlik isteklerini ve kendi güvenlik biriminin ID'sini (SAID) gönderir.

Üçüncü aşama: eğer BS, SS tarafından gönderilen sertifikayı onaylarsa bir asıllama anahtarı(Authentication Key-AK) üretir. Ürettiği bu AK'yı SS'in sertifikasından elde ettiği RSA tabanlı açık anahtarla şifreler. Bununla birlikte anahtar yaşam süresi[4], SS'in isteklerine karşı verilebilcek güvenlik cevapları ile AK'nın sekans numarası[5] da SS'e gönderililir.

Bu üç aşamalı mesajlaşmadan sonra(ilk aşama tek taraflı diğer aşamalar çift taraflı olmak üzere) SS kendisini BS'e asıllandığının kanıtı olan AK'yı elde etmiş olur.

Şekil-5 sözü edilen asıllamanın ikinci ve üçüncü aşamaları göstermektedir.



Şekil-5
Asıllama anahtarı (AK) istek-cevap diyagramı

ii. Anahtar yönetimi

Anahtar yönetimi asıllama ve veri şifreleme anahtarlarının oluşumu ve bu anahtarların alışverişi anlamına gelmektedir. Bu yönetim güvenlik altkatmanında Privacy Key Management (PKM) ile sağlanmaktadır. PKM ayrıca oturum tazeleme[6] işlemlerini de yürütür. PKM güvenlik birimi tarafından yönetilmektedir. SS'ler, PKM protokolünü BS'den asıllama ve trafik güvenliği parametrelerini almak için kullanır.

[4] Anahtar yaşam süresi 1-70 gün arasındadır.
[5] AK'nın sekans numarası üretilen kaçıncı AK olduğunu belirtir.
[6] Oturum tazeleme, periyodik aralıklarla AK'nın yeniden gönderilmesine dayanır.

AK oluşumu ve SS'e iletilmesinden sonra, veri şifrelenmesinde kullanılcak olan Traffic Encryption Key (TEK) oluşumu ve iletimine geçilir.TEK, bir DES anahtarlamasıdır ve 56 bittir. TEK'in oluşumu ve gönderilmesinde AK'dan yararlanırlır. TEK üç değişik şekilde BS'ten SS'e gönderilir:

112-bitlik KEK anahtarı yardımıyla 3DES kullanılarak
128-bitlik KEK anahtarı yardımıyla AES kullanılarak
SS'in açık anahtarı yardımıyla RSA kullanılarak

AK burada, TEK oluşumunda kullanılan Key Encryption Key (KEK) yapımını sağlar. KEK, 112 yada 128 bit olabilir.

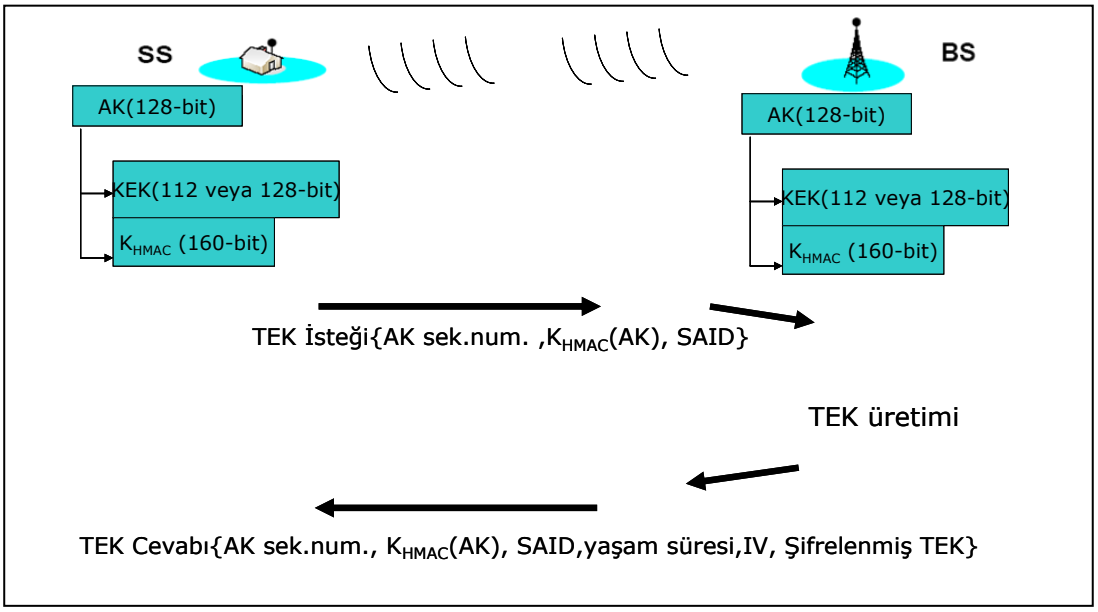
Ayrıca veri bütünlüğü ve asıllama amaçlı kullanılcak olan bir öz alma fonksiyonunda (HMAC) yer alması gereken K anahtarı da AK'dır. Kullanılan öz alma fonksiyonu HMAC-SHA1'dir.

Asıllama gerçekleştiksen sonra veri şifrelenmesi için kullanılacak olan TEK anahtarının SS tarafından elde edilmesinin aşamaları şu şekildedir:

Birinci aşama: SS, BS'e, kendisinde bulunan AK'nın sekan numarasını,güvenlik biriminin ID'sini (SAID) ve AK'nın HMAC-SHA1 ile alınmış özünü gönderir.

İkinci aşama: BS, SS'den aldığı AK'nın özünü alır ve kendisine gelen öz ile karşılaştırır.Eğer bunlar tutuyorsa, karşısındaki biraz önce asıllamasını yaptığı SS'tir. Bunu anladıktan sonra rastgele bir biçimde TEK üretir(128-bit). Daha sonra SS'e kendisine gelen AK'nın sekans numarasını,kendi SAID'ini, yine yukarıda anlatılan üç methoddan biriyle şifrelenmiş TEK'i, TEK anahtarının yaşam süresini[7], başlangıç vektörünü ve AK'nın özünü gönderir. Bunları alan SS, eğer özler tutuyor ise TEK'i kabul eder ve şifreli veri aktarımına başlar.

Şekil-6 bu iki aşamayı göstermektedir.



Şekil-6
TEK istek-cevap diyagramı

[7] TEK yaşam süresi 30 dakika ile 7 gün arasındadır.

e. 802.16 Örgü (Mesh) Yapılarda Güvenlik Unsurları

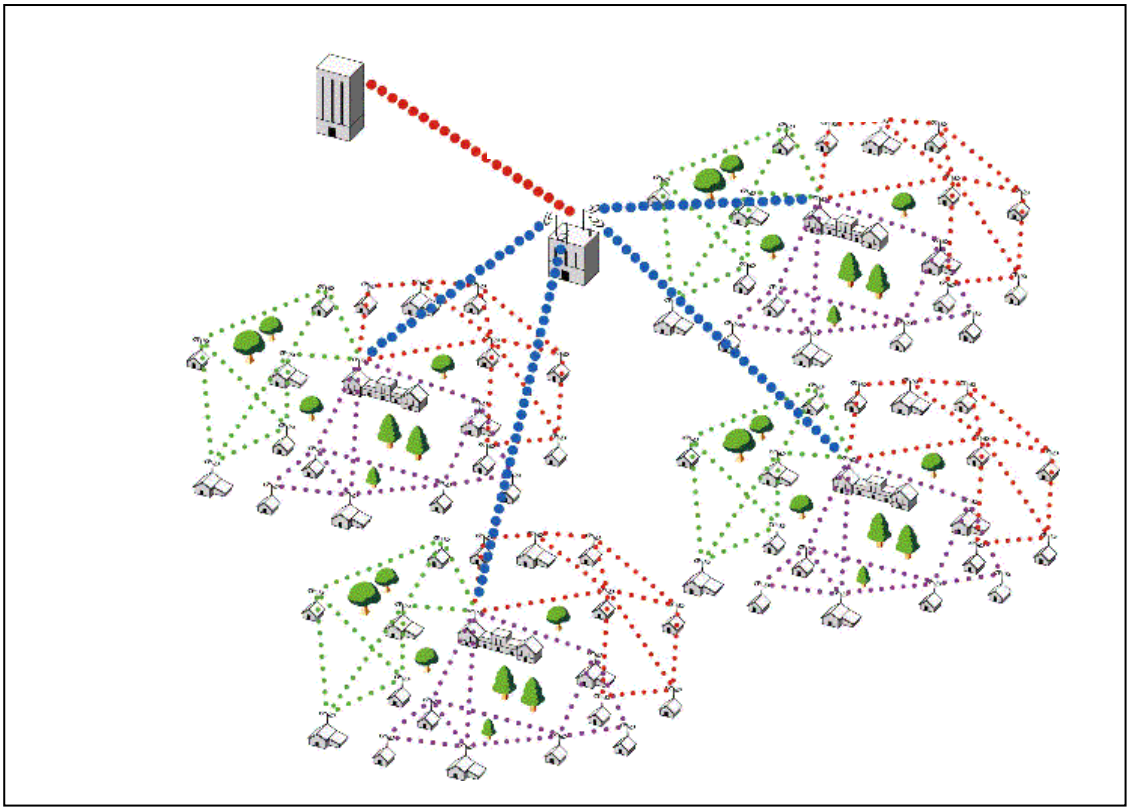
802.16'nın çalışma kiplerinden biri de Örgü kipidir. Şekil-7 tipik bir merkezi örgü ağını göstermektedir. Burada her ev bir SS olarak düşünülmüştür. SS'lerden sadece belli bir tanesi BS ile iletişimde olup diğerleri kendi aralarında doğrudan bir bağlantı kurabilirler.
Örgü kipinin WiMAX yapısında kullanılmasının sağladığı belli başlı yararlar şu şekilde sıralanabilir:

- SS'lerin doğrudan BS ile bağlantı kurma zorunlulukları ortadan kalkar. Bu şekilde olunca bir SS'nin sisteme katılması, veri alışverişi ve sistemden ayrılması için geçecek olan süre azalacaktır. Ayrıca SS-BS arası gidip gelen kontrol mesajları ve tazeleme mesajları da olmayacagından sistemdeki trafiğin yaratabileceği gürültü ve girişim azalır.

- Ayrıca BS'in tüm SS'lere ulaşması gerekmediğinden, oluşturulan ağın çapı genişletilmiş olacaktır. WiMAX ağının çapının genişlemesi, kapsama alanındaki genişleme olarak düşünülebilir.

- Sistemde BS çöktüğünde, PMP yapısındaki bir WiMAX ağında iletişim tamamen dururken, örgü yapısında iletişim tamamen kopmaz. Aynı şekilde bir SS'in çekmesi, PMP kipinde çalışmada daha uzun sürede çözülen bir sorunken, örgü ağlarında bu sorun başka bir yol bulmanın kolaylığından ötürü daha çabuk üstesinden gelinir.

Örgü ağlarıyla sağlanan bu avantajlar beraberinde bir takım güvenlik eksiklikleri de getirmektedir.



Şekil-7
Merkezi örgü (Centralized Mesh) 802.16 ağ yapısı

WiMAX-Örgülü yapılarda güvenlik aşamaları şu şekildedir:

- Mesh ağına katılmak isteyen bir düğüm kendisine en yakın düğümü "sponsor düğüm" ilan eder.
- İstemci düğüm,kendisini asıllaması için sponspor düğüme mesaj gönderir.
- PMP'teki güvenlik işlemlerinin benzeri sponsor düğüm tarafından yapılır. Sponsor düğüm, sertifikalarını dağıtıldığı kurumdan, ağa katılmak isteyen SS'in sertifikasını edinir(eğer sertifikası var ise bunu doğrular). Daha sonra kendisini asıllayan düğümle iletişime geçerek sanki kendisini bir daha asıllıyormuş gibi ağa katılmak isteyen düğümün asıllama işlemlerini, gerçekleştirir.
- Asıllama işini yapan gerçek düğümle bir tünel kuran elçi düğüm, istemci düğüme mesajları iletir. Bir önceki aşamadaki mesajlar artık bu tünel aracılığıyla ağa katılmak isteyen düğüme gönderilir.
    - Asıllama mesajları
    - Anahtar alışverişi
- Mesh'e dahil olan düğüm, diğer düğümlerle iletişime geçebilir.

3. ALTYAPININ ANALİZİ

İkinci bölümde incelenen 802.16 güvenlik altyapısı, artan güvenlik istekleri, geliştirilen yeni algoritmalar,asıllama protokolleri, anahtar değişim mekanizmaları vb. yüzünden bir çok eleştiriye maruz kalmıştır. Standard, bu haliyle güvenlik anlamında güçsüzleşmektedir. Özellikle 2 düzeyde incelenen veri şifrelemesi,asıllama ve anahtar yönetimi konularında karşılaşılabilcek sorunlar ve bunlar için önerilen çözümler incelenebilir.

a. Veri Şifrelemesindeki Sorunlar

Veri şifreleme CBC-DES algoritmasıyla yapılmaktadır. DES algoritması günümüzde deneme-yanılma veya Brute-Force yöntemleriyle kırılabilir bir algoritmaya dönüşmüştür. Bunun yerine yine bir simetrik anahtarlı kriptografi olan AES algoritmasına geçilebilir. 128-bitlik bir AES oluşumuna gidilirse 64-bitlik DES'ten daha iyi bir güvenlik sağlanacağı açıktır. Güvenlikle birlikte gelen hız problemine rağmen DES algoritmasının kolay çözülebilir yapısından AES'in güvenli yapısına geçiş yapılabilir.

Ağ güvenliğinin önemli problemlerinden olan tekrar saldırıları 802.16 tabanlı ağlarda da rahatca gerçekleştirilebilir. Özellikle telsiz ağın doğasından kaynaklanan "sinyali ele geçirebilme ve dinleyebilme" özelliği, sadece pasif değil aktif saldırılarında oluşması olasılığını doğurur. Bunu engellemek için veri şifrelemesi sırasında tekrar saldırılarını engelleyecek rastgele sayı üretimi yöntemi kullanılabilir. Dikkat edilecek olursa, ne AK anahtarının değişiminde, ne TEK anahtarının değişiminde ne de asıllamalarda, herhangi bir şekilde SS, sadece kendisinin üretebileceği rassallıkla sayılar üretme yoluna gitmemektedir.Tekrar saldıralına elverişlilik katan bu zemin, protokole eklenecek bir rastgele sayı üretimi, paket sekans numaralarının koyulması şeklinde çözülebilir.

Veri şifrelemede ortaya çıkan bir diğer sorun kullanılan şifreleme kipininden kaynaklanmaktadır. CBC kipi, bir başlangıç vektörü gerektirir. Bu vektör TEK alışverişi sırasında öğrenilir. Tahmin edilebilecek bir yapıya sahip olan bu vektör seçilen açık metin saldırlarına karşı sistemi dayanıksız kılar. Belirli zamanlarda ortamdan paketleri alan kötü niyetli bir kişi, elde ettiği verilerden esas metine ulaşabilir. Başlangıç vektöründeki bu sorunun çözümü olarak bu vektörün her bir metin için değil, her bir MAC çercevesi için üretimi düşünülebilir. Bu şekilde araya giren kötü niyetli kişi, seçilen açık metin saldırısı yapsa dahi tam olarak metni yada anahtarı elde etme olasılığı önceki seçeneğe göre çok azalmıştır. Başka bir çözüm de bu vektörün ayrı olarak değilde veriye gömülmesi şeklinde olabilir. Bu durumda karşılaşılabilecek problem şifreleme yükünün artmasıdır. Çünkü şifrelenecek veriye birde başlangıç vektörü eklenmiştir.

b. Anahtar Yönetimindeki Sorunlar

Veri şifrelemesinde kullanılan TEK anahtarının sekans numarası 2 bittir. Bu 4 değişik sekans numaralı TEK oluşumu anlamına gelir. Eğer bir tekrar saldırısı yapılır ve başarılı olunur ise, bu tekrar saldırısından TEK'i cıkartma olasılığı da ¼ mertebesindedir. Tekrar saldırılarına karşı çok güvenli bir sistemde olunmadığı hatırlacak olursa ,veri şifrelemede kullanılacak kritik TEK anahtarının kolayca elde edilebileceği sonucuna varılır.

Standarttaki başka bir açık ise, TEK'in üretildiği rassal fonksiyon hakkında kesin bir bilgi verilmemesidir. Bu sayede her BS kendine özgü bir yerel fonksiyon kullanarak TEK üretebilir. Standartlarda belirtilmemiş ve tamamen üretici firma tabanlı çözümlere gidilen bu metod, ağda güvensizlik ve dengesizlik gibi problemler ortaya çıkarabilir.

Standartta belirtilene göre, BS tarafından oluşturulan AK'nın yeni üretildiği konusunda SS'in tek güvencesi onun BS'ten gelmesidir. Buradan da anlaşılabiliceği gibi, BS'e tam bir güven söz konusudur. Olasi bir "kötü niyetli BS" oluışumu, sistemin tamamen çökmesine ya da kötü niyetli kişinin amacına yönelik olarak çalışmasına sebep olur. SS'in BS tarafından gönderilen AK'nın tazeliğine bakabilecek bir yapı oluşturulabilmesi bu konudaki eksikliği kapatacaktır.

c. Asıllamadaki Sorunlar

Standartta belirtilen asıllamadaki en temek problem asıllamanın tek yönlü yapılamasıdır. Günümüz asıllama protokollerinde karşımıza çıkan "X olduğunu iddea ediyorsun, kanıtla!" felsefesi burada kullanılmamaktadır. Burada asıllanan sadece SS'tir. SS gönderdiği sertifika ile kendisinin onaylı açık anahtarını BS'e iletmekte ve kendini BS'e asıllamaktadır. BS benzeri bir şekilde davranmamakta sadece SS'i tanıdığını ve asılladığını belirtmektedir. Asıllama protokollerinin tasarımında temel unsurlardan olan karşı taraf sormadan kendini asıllamama felsefesi kullanılmadığı için ortaya çıkan bu açık, bir ortadaki adam (Man-In-The-Middle-Attack) saldırısına karşı savunmasız hale gelmektedir.

Asıllama protokolünde doğrulama için gönderilen mesajlar yetersizdir. Gönderilen SAID, araya giren bir tekrar saldırısı ile klonlanabilir. Günümüzde yaygınlaşan bir asıllama protokolü olan Extensible Authentication Protocol (EAP) tabanlı bir asıllama

felsefesi geliştirebilir. Özellikle EAP-TLS (EAP with Transport Layer Security) ve EAP-MD5 (öz almaya dayalı asıllama) ile daha güçlü asıllama yapılabilir.

Bundan başka bir sorun olarak, standartta sertifika otoriteleri hiyararşisi hakkında hiç bilgi verilmemektedir. Bu konu, özellikle X.509 temelli bir sertifikalandırma yapan sistemlerde soruna sebep olabilir. Standartta hangi kök otoritesinden hangi bölgesel otoritelere nasıl bir hiyararşi izlenerek sertifika doğrulaması yapılması gerektiği söylenmelidir.

4. SONUÇ

IEEE, 802.11 standardıyla birlikte temellerini attığı telsiz iletişimde 802.16 ile bir üst noktaya ulaşmıştır. 802.16'da ki 2 düzeyli moduler güvenlik altyapı desteği, tamamen protokol tabanlı olan ve katmanlı bir yapıya sahip olmayan 802.11'e kıyasla geliştirilmeye daha elverişli bir altyapı olarak ortaya çıkmaktadır.

Standartta söylenen veri şifreleme algoritması(DES), veri şifreleme kipinde kullanılan vektörün tahmin edilebilirliği, tekrar saldıralarına karşı savunmasızlık ve tek yönlü asıllama yapılması gibi temel problemler 802.16 WiMAX tabanlı ağlarda da kullanıcının karşısına çıkmaktadır. Ayrıca standartlarda tam açık olarak belirtilmeyen noktalar güvenlikte dengesizlik ve kararsızlıklar getirebilmektedir. Günümüz teknolojisiyle,standarttaki açıklar kapatılmaya başlanmıştır(DES yerine AES kullanımı, asıllama protokolü olarak EAP kullanımı vb.) .

Yapılan bu çalışma ile 802.16 WiMAX'ın 802.11'e göre katmanlı bir yapıya sahip olmasından ötürü güvenlik sorunlarının bulunup çözümünde bir avantajı olsa da, hala üzerinde konuşulması gereken bir konu olduğu sonucuna varılmıştır.

5. YARARLANILAN KAYNAKLAR

[1] IEEE Std 802.16-2004--IEEE standard for local and metropolitan areanetworks, part 16: "***Air Interface for Fixed Broadband Wireless Access Systems***".

[2] David Johnston ve Jesse Walker--INTEL: "***Overview of IEEE 802.16 Security***"

[3] Kitti Wongthavarawat--Thai Computer Emergency Response Team (ThaiCERT) National Electronics and Computer Technology Center,Thailand: "***IEEE 802.16 WiMax Security***"

[4] Loutfi Nuaymi, Patrick Maillé, Francis Dupont, Raphaël Didier--École Nationale Supérieure des Télécommunications de Bretagne:"***Security issues in WiMAX/IEEE 802.16 BWA System***"

[5] Yun Zhou ve Yuguang Fang--Department of Electrical and Computer Engineering,University of Florida, Gainesville:"***Security of 802.16 in Mesh Mode***"

[6] William Stallings, ***Data and Computer Communications***, network Security, sayfa 707-74, Prentice Hall,2002

[7] Theodore Rappaport, ***Wireless Coımmunications principles and practice***, Linear Modulation Techniques, sayfa 294-308, Prentice Hall,2002

[8] WiMAX forum-- http://www.wimaxforum.org

[9] WiMAX Türkiye-- http://www.wimaxturkiye.com

[10] WiMAX Intel--http://www.intel.com/netcomms/technologies/wimax/index.htm

[11] The IEEE 802.16 Working Group on Broadband Wireless Access Standards-- http://www.ieee802.org/16/