İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi Yıl: 8 Sayı: 16 Güz 2009/2 s. 31-46

AES -TURBO VE AES -TURBO-OFDM SİSTEMLERİNİN BİT HATA ORANI KARŞILAŞTIRILMASI

Volkan ÖZDURAN*, Hakan ÇAM#, Osman Nuri UÇAN*

Geliş: 22. 06.2009 Kabul: 18.01.2010

ÖZET

Haberleşme sistemleri üzerindeki gelişmeler, araştırmacıları daha etkili ve güvenli haberleşme sistemleri üzerine çalışmaya zorlamaktadır. Bu çalışmada klasik haberleşme sistemlerinden farklı olarak çeşitli kodlama teknikleri kullanarak daha verimli haberleşme verileri elde etmek amaçlanmıştır. İleri şifreleme tekniği (AES) kullanılarak bit dizisi şifrelenmiştir. Derin uzay haberleşmesinde ve 3G haberleşmesinde kullanılan Turbo Kodlayıcı ve Turbo Kod Çözücü sistemleri kullanılmıştır. Daha verimli ve daha düşük Sinyal/Gürültü Oranında(SNR) etkili haberleşme imkanı sağlamak için Dik Frekans Bölmeli Çoğullama (OFDM) Sistemi kullanılmıştır. OFDM sistemleri cep telefonlarının, baz istasyonu ile yaptığı iletişim sırasında daha az güç harcamasını sağlamaktadır. Yine OFDM sistemleri uydu haberleşmesi sırasında uplink ve downlink haberleşmesi sırasında kullanılmaktadır. Bu çalışmada, Beyaz Gauss Gürültüsü eklenmiş(AWGN) ortamda, AES şifreleme tekniği ile şifrelenmiş Turbo Kodlayıcı ile kodlanmış sistem ile elde edilen performans eğrileri ile bu sistemin sonuna eklenmiş olan Dik Frekans Bölmeli Çoğullamalı sistem ile elde edilen performans eğrileri karşılaştırılmıştır. OFDM'in bu sistemin performansına olan etkisi araştırılmaya çalışılmıştır.

Anahtar Kelimeler: İleri Şifreleme Standardı(AES),Turbo Kodlama, Dik Frekans Bölmeli Çoğullama(OFDM), Beyaz Gauss Gürültüsü (AWGN)

BIT ERROR RATE COMPARISON OF AES-TURBO AND AES-TURBO-OFDM SYSTEMS

ABSTRACT

The developments on the telecommunication systems urge the researchers to study on more efficient and secure communication systems. In this study, apart from the traditional communication systems it is purposed to obtain more efficient telecommunication data by utilizing various coding techniques. The bit sequence is encrypted by using an Advanced Encryption Standard (AES) Technique. Turbo Encoders and Turbo Decoder systems which are used in deep space communication and 3G communication are implemented here. In order to provide an effective telecommunication capability with more efficient and lower Signal to Noise Ratio (SNR), an Orthogonal Frequency Divided Multiplexing (OFDM) has been implemented. OFDM systems allow consuming less power for the telecommunication amongst the Cell-phones and base stations. And also, OFDM systems are used in uplink and downlink communication of satellite communications. In this study, in an environment of Additive White Gaussian Noise (AWGN), the performance curves which are obtained by using a system encrypted with a Turbo encoder by means of an AES encrypting system have been compared to the performance curves which are obtained by means of Orthogonal Frequency Divided Multiplexing system. It has been studied to investigate the effect of OFDM on the performance of such system.

Keywords: Advanced Encryption Standard(AES),Turbo Coding, Orthogonal Frequency Division Multiplexing(OFDM), Additive White Gaussian Noise (AWGN).

* *İstanbul Üniversitesi, Mühendislik Fakültesi, Elektrik-Elektronik Mühendisliği Bölümü, Avcılar-İstanbul, uosman@istanbul.edu.tr, volkan@istanbul.edu.tr .*

Hava Harp Okulu, Yeşilköy, İstanbul.

1. GİRİŞ

Bu çalışmada bir haberleşme sisteminin verici kısmında, AES şifreleme tekniği (Daemen ve Rijmen,1999) kullanılarak elde edilen karmaşık bit dizisi Turbo Kodlayıcı bloğuna verilmiştir. Turbo Kodlayıcının çıkışından alınan bit dizisi BPSK ile modüle edilerek OFDM bloğuna verilmiştir. OFDM verici bloğunun çıkışında elde edilen veriler kablosuz kanala gönderilmiştir. Kanal modeli olarak Beyaz Gauss Gürültüsü eklenmiş (AWGN) kanal modeli seçilmiştir.

Söz konusu haberleşme sisteminin alıcı kısmında ise verici kısmında yapılan işlemlerin tersi işlemler yapılmıştır. İlk olarak AWGN kanaldan alınan gürültülü sinyal OFDM alıcı bloğuna girilir. Alıcı kısmında bulunan OFDM bloğunda verici kısmında yapılan işlemlerin tersi işlemler yapılır. OFDM bloğunun çıkışı BPSK ile ters modülasyon işleminden sonra Turbo Kod çözücü bloğuna verilir. Son adımda elde edilen bit dizisi AES şifre çözücü bloğuna verilir. Bu şekilde sistemin performansı ölçülmeye çalışılmıştır.

Daha önceki yapılan çalışmalarda, (Özduran, 2008), (Özduran vd., 2008) çalışmasında ayrık bloklar halinde AES ve Turbo Kodlayıcının AWGN kanaldaki performansları incelenmiştir. (Mahmood, 2008) çalışmasında performansın arttırılması için şifreleme işlemi kod çözücünün içerisinde yapılarak sonuca gidilmeye çalışılmıştır. (Arnone vd., 2009) çalışmasında AES ve Turbo Kodlayıcının birleşik halde olduğu bir sistem üzerinde çalışılmıştır. (Çam vd.,2010) çalışmasında çok seviyeli AES kullanılmıştır. Turbo Kodlayıcıdan farklı bir kanal kodlayıcı yapısı mevcuttur. Farklı bir modülasyon tekniğine yer verilmiştir. Kanal modeli olarak Kablosuz Sensör Ağlar üzerinden haberleşme yapılmaya çalışılmıştır. Bu çalışmada ise ayrık bloklar halinde olan AES ve Turbo Kodlayıcıya ek olarak sisteme OFDM eklenerek sistemin performansı incelenmeye çalışılmıştır. Şifrelenmiş, Turbo Kodlanmış OFDM sistemi ile sadece şifrelenmiş ve Turbo Kodlanmış sistemin birbirine olan üstünlükleri belirlenmeye çalışılmıştır.

Aşağıdaki bölümlerde söz konusu haberleşme sisteminde kullanılan bloklar anlatılmıştır. Sistemin genel blok diyagramına yer verilmiştir. Simülasyon kısmında ise MATLAB paket programı kullanılarak söz konusu haberleşme sistemi modellenmiştir. OFDM verici bloğundan sonra elde edilen bit dizilerinin dağılımı şekil üzerinde gösterilmiştir. Yine OFDM verici bloğundan sonra bit dizisi AWGN kanala gönderilmiştir. Sinyalin üstüne AWGN gürültüsü eklendikten sonra elde edilen gürültülü sinyalin grafiğine yer verilmiştir. OFDM alıcı çıkışında elde edilen sinyalin bölgesel dağılımına yer verilmiştir. Simülasyon kısmında son olarak AES-TURBO-OFDM sistemi kullanılarak çeşitli SNR değerlerinde elde edilen verileri kullanılarak elde edilen performans eğrileri ile AES-TURBO sistemi kullanılarak elde edilen performans eğrileri karşılaştırılmıştır. OFDM'in sistemin performansına olan etkisi incelenmeye çalışılmıştır.

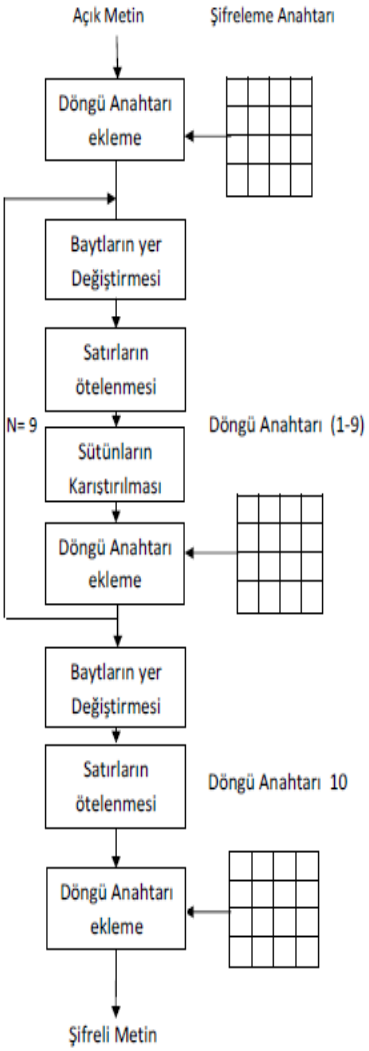
2. AES (İLERİ ŞİFRELEME STANDARDI)

Simetrik şifreleme grubuna dahil olan AES (İleri Şifreleme Standardı) algoritması 128 bit veri bloklarını 128,192 ve 256 bit anahtar seçenekleri ile şifreleyen bir şifreleme algoritmasıdır. Döngü sayısı anahtar genişliğine göre değişmektedir. 128 bit anahtar için 10 döngüde şifreleme yaparken 192 ve 256 bit anahtar uzunluğu için sırasıyla 12 ve 14 döngüde şifreleme yapmaktadır. AES kullandığı anahtar boyutuna göre "AES-128" , "AES-192" ve "AES-256" olarak da adlandırılır.

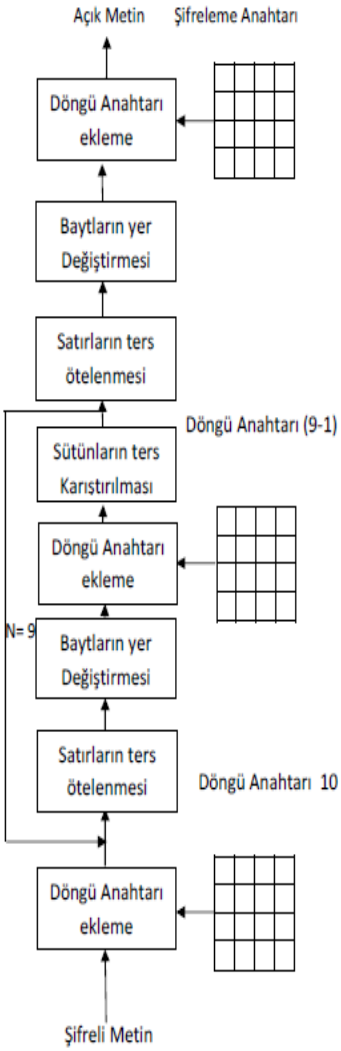
Şifreleme işleminde ilk olarak 128 bit veri 4x4 byte matrisine dönüştürülür. Daha sonra her döngüde sırasıyla byte'ların yer değiştirmesi, satırların ötelenmesi, sütünların karıştırılması ve anahtar planlamadan gelen o döngü için belirlenen anahtar ile XOR'lama işlemleri yapılır. Byte'ların yer değiştirilmesinde 16 byte değerinin her biri 8 bit girişli 8 bit çıkışlı S kutusuna sokulur. S kutusu değerleri, Galois cisiminde (Galois Field-GF) GF(2^8), 8 bitlik polinom için ters alındıktan sonra doğrusal bir dönüşüme sokularak elde edilmiştir. Satırların ötelenmesi işleminde 4x4 byte matrisinde satırlar ötelenir ve sütunların karıştırılması işleminde herhangi bir sütun için o sütundaki değerler karıştırılır. Döngünün son katmanında ise o döngüye ait anahtar ile XOR'lama yapılmaktadır. (FIPS 197, 2001), (Sakallı, 2006).

AES şifre çözme işleminde ise şifreleme işleminde yapılan işlemlerin tam tersi yapılarak şifrelenmiş verinin şifresi çözülür.

Aşağıdaki şekilde 128 bit anahtar boyutu seçilerek, AES şifreleme ve şifre çözme algoritmasının geniş bir gösterilimi mevcuttur.



Şekil 1. AES Şifreleme Bloğu



Şekil 2. AES Şifre Çözme Bloğu

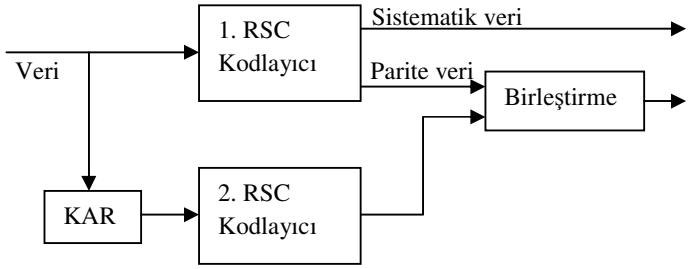
3. TURBO KODLAR

Turbo Kodlama tekniği, yapısal olarak ardışık kodlama tekniğinin geliştirilmiş bir versiyonu ile kod çözme için kullanılan bir iteratif kod çözme algoritmasından ibarettir. Turbo Kodlamanın temel unsurlarından biri olan ardışık kodlama, ilk olarak Forney tarafından tasarlanmış bir tekniktir. Bu teknik,

iki ya da daha fazla basit kodlayıcının, yüksek kod kazancına ulaşabilmek için paralel yada seri birleştirilmesinden oluşmaktadır. Turbo Kodlar Shannon'un (Shannon,1948) bit hata oranı limit değerine yaklaşmıştır.(Berrou vd. 1993) Netice de ortaya çıkan bu konular, çok uzun kodların hata düzeltme kabiliyetlerine sahip olmakla birlikte onlara göre daha makul sayılabilecek karmaşıklıkta bir kod çözme yapısına sahiptirler (Osman ve Uçan, 2006).

3.1. Turbo Kodlayıcı

Turbo Kodlayıcının genel yapısı Şekil 3'te verilmiştir. Turbo Kodlayıcı iki tane genellikle aynı yapıdaki geri beslemeli sistematik katlamalı (RSC) kodlayıcıdan oluşur. Her iki kodlayıcıda aynı bilgiyi alır. Fakat ikinci kodlayıcı giriş bilgisi karıştırıcıdan geçtikten sonra oluşan yeni dizilimli bilgiyi alır. Turbo Kodlarının rasgele gibi görünmesini sağlayan bu karıştırma işlemidir. Eğer karıştırıcının boyutu sabit ve her iki RSC kodlayıcının başlangıç durumları sıfırsa, bu durumdaki Turbo Kodlara lineer blok kodlar denir. (Osman ve Uçan, 2003), (Osman ve Uçan, 2006), (Berrou vd.,1993), (Osman,2004).

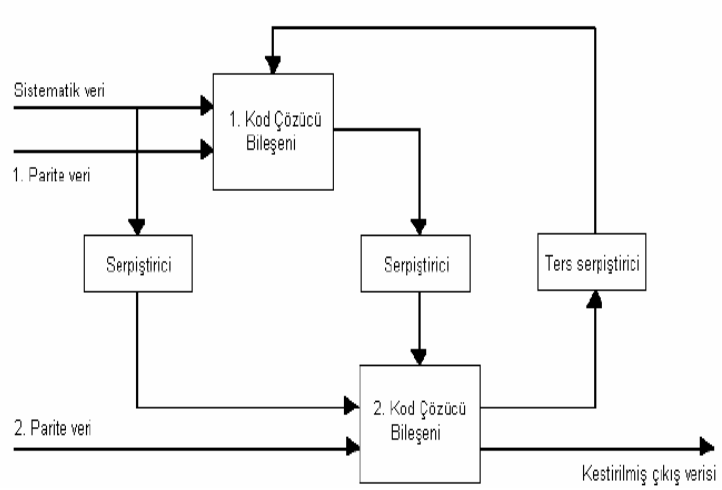


Şekil 3. Turbo Kodlayıcı

3.2. Turbo Kod Çözücü

Şekil 4'teki kod çözücü iteratif bir çalışma sistemine sahiptir. İlk iterasyonda 1. kod çözücü bileşeni, sadece kanal çıkışlarını alır ve veri bitlerinin tahmini değerini veren bir soft çıkış üretir. 1. kod çözücü bileşeninin ürettiği bu soft çıkış bilgisi, ikinci kod çözücü bileşeni tarafından ek bilgi olarak kullanılır. İkinci kod çözücü bu bilgiyi kanal çıkışlarıyla birlikte veri bitlerinin tahminini oluşturmak için kullanır. Buraya kadar yapılan işlemler birinci iterasyona aittir. Daha sonra ikinci iterasyon başlar ve ilk kod çözücü yine kanal çıkışlarını kullanarak kod çözme işlemini gerçekleştirir. Fakat ikinci iterasyonda, sadece kanaldan alınan bilgileri değil, ilk iterasyonda ikinci kod çözücünün ürettiği giriş bitleri hakkındaki ek bilgiyi de kullanır. Bu fazladan bilgi, 1. kod çözücü bileşeninin daha gerçek soft çıkışlar oluşturmasını sağlar. Daha sonra bu çıkışlar da ikinci kod çözücü tarafından önsel bilgi olarak kullanılır. Bu döngü bu şekilde devam eder ve her iterasyonda kodu çözülen bitlerin BER değeri gitgide düşer.

İterasyon sayısının yükseltilmesi ile oluşturulan performans gelişimi, iterasyon sayısı arttıkça daha az gerçekleşir. Ayrıca kod çözücünün karmaşık yapısı, iterasyon sayısının çok fazla olmasına müsaade etmeyecektir. Bu nedenle iterasyon sayısı genellikle 8-10 civarında seçilir. (Osman ve Uçan, 2003), (Osman ve Uçan, 2003), (Osman,2004).



Şekil 4. Turbo Kod Çözücü'nün Yapısı

4. OFDM

Ortogonal Frekans Bölmeli Çoğullama (OFDM), yüksek hızlı bir veriyi düşük hızlı çok sayıdaki ortogonal alt taşıyıcılar üzerinden ileten özel çok taşıyıcılı bir iletim şeklidir. Bütün taşıyıcılar birbirine göre ortogonal olduklarından OFDM, kanalları birbirine daha yakın yerleştirmek suretiyle tayfı daha verimli kullanabilmekte; böylece yakın yerleştirilen taşıyıcılar arasındaki girişim önlenebilmektedir. OFDM'nin tercih edilme sebeplerinden birisi, frekans seçici sönümleme ya da dar band girişime karşı direnci artırmaktır. Tek taşıyıcılı bir sistemde, bir sönümleme ya da girişim hattın tamamının zayıflamasına neden olurken, çok taşıyıcılı bir sistemde alt taşıyıcıların sadece küçük bir yüzdesi bu durumdan etkilenmektedir (Van Nee ve Prasad, 2000),(Heiskala ve Terry, 2001), (İmamoğlu ve Taşpınar, 2004).

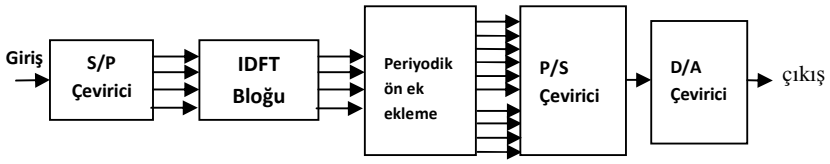
İlk ortaya atıldığında atıl bir teknik olarak görülen OFDM'e gösterilen ilgi, son yıllarda, özellikle sayısal veri işleme tekniklerinde ve bunların pratiğe uygulanmasını mümkün kılan tümleşik devrelerin geliştirilmesinde kaydedilen ilerlemeler sayesinde fazlaca artmıştır.

Artan bu ilginin son göstergesi, OFDM'in IEE802.11a ve ETSI BRAN gibi standartlar tarafından telsiz yerel alan ağlar (WLAN) için, yüksek hızlı veri iletimi konusunda en güvenilir modülasyon tekniği olarak seçilmesidir (Koraltürk, 2008).

4.1. OFDM'in Verici Ve Alıcı Yapıları

4.1.1. OFDM Verici Yapısı

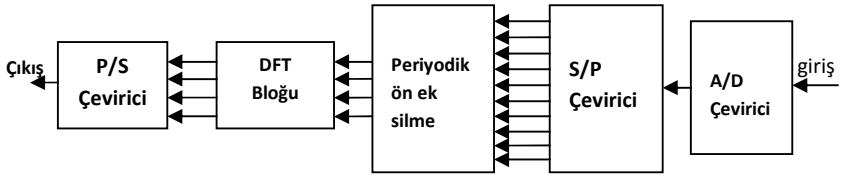
Şekil 5'te OFDM sisteminin verici yapısı gösterilmiştir. Veri girişi kısmından OFDM bloğuna bit dizisi gönderildiğinde Seri/Paralel çevirici bloğu ile vektör halde bulunan bit dizisi matris haline dönüştürülür. IDFT bloğu kullanılarak alt taşıyıcılar üretilir. Periyodik ön ek ekleme bloğu ile bit dizisinin sonundaki bitler başa eklenerek semboller arası girişim (ISI) ve taşıyıcılar arası girişim (ICI) etkileri ortadan kaldırılmaya çalışılmıştır. Paralel/Seri çevirici bloğu ile matris halindeki bit dizisi vektör haline dönüştürülür (Litwin ve Pugel, 2001), (Engels, 2002).



Şekil 5. OFDM Verici Yapısı

4.1.2. OFDM Alıcı Yapısı

OFDM alıcı bloğunda, OFDM verici bloğundaki yapılan işlemlerin tam tersi yapılır. Kanaldan seri halde alınan bit dizisi Seri/Paralel çevirici vasıtasıyla matris haline dönüştürülür. Periyodik ön ek silme bloğu ile verici kısmında semboller ve taşıyıcılar arası girişimi engellemek için eklenen bitler silinir. DFT bloğundan geçirildikten sonra Paralel/Seri dönüştürücü sayesinde seri bir çıkış alınır. (Litwin ve Pugel, 2001), (Engels, 2002).



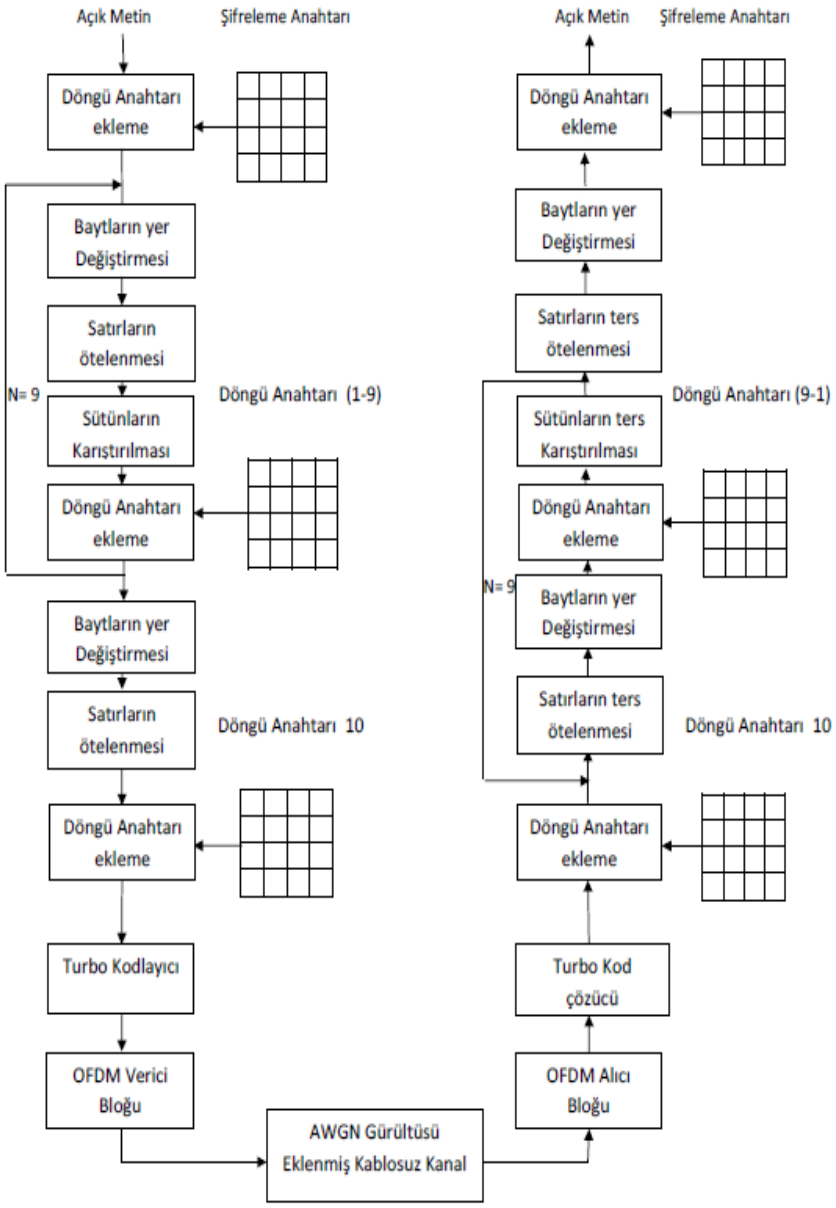
Şekil 6. OFDM Alıcı Yapısı

5. SİMULASYON SONUÇLARI

AES-TURBO çalışmasında (Özduran, 2008), (Özduran vd., 2008) yapılan AES (İleri Şifreleme Tekniği) şifreleme tekniği kullanılarak Turbo Kodlayıcı'dan geçirilerek AWGN kanal tipinde elde edilen performans eğrileri ile OFDM'in bu sistemin performansına olan etkisinin araştırılması amaçlanmıştır. Bunun için 128 bit uzunluğunda bit dizisi seçilmiştir. AES şifreleme tekniği ile şifreleme işlemi yapılırken 128 bit uzunluğunda anahtar seçilmiştir. Şifreli metini elde ettikten sonra bit dizisi Turbo Kodlayıcıya verilir.

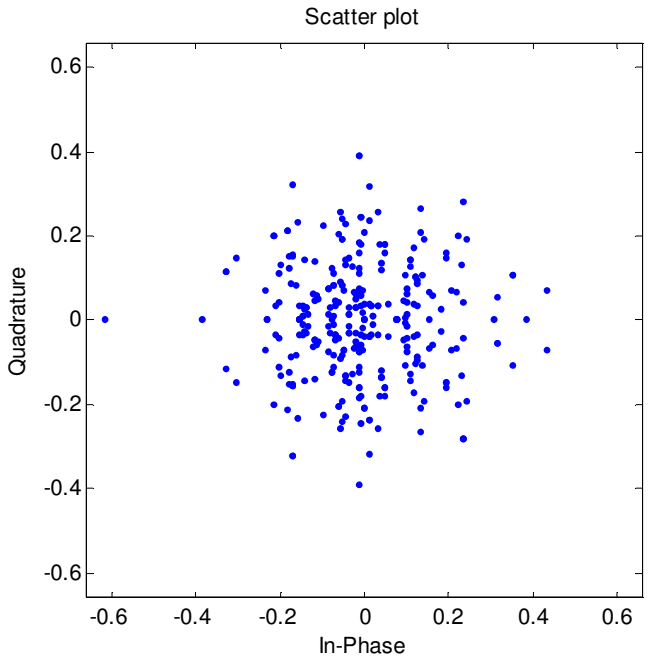
Turbo Kodlayıcı çıkışında kuyruk bitleri ile birlikte toplam 260 bit çıkış elde edilir. 260 bit uzunluğundaki veri BPSK ile modüle edilerek OFDM verici bloğunda gönderilir. Buraya seri bir şekilde gelen bit dizisi IDFT bloğuna gönderileceği için seriden paralel hale dönüştürülür. IDFT bloğundan geçtikten sonra bit dizisi periyodik ön ek ekleme bloğuna gelir. Kanala seri bir şekilde gönderileceği için paralel halde bulunan bit dizisi seri hale getirilir. OFDM çıkışında elde edilen bit dizisinin dağılımı Şekil 8'de gösterilmiştir.

OFDM'in verici kısmında elde edilen sinyal AWGN kanala gönderilir. Burada sinyalin üzerine AWGN gürültüsü eklenir. AWGN gürültüsü eklenmiş hali Şekil 9'da gösterilmiştir. Alıcı kısmında ise verici kısmında yapılan işlemlerin tam tersi yapılır. Seri halde gelen gürültülü sinyal paralel hale dönüştürülür. Verici kısmında kanaldaki semboller arası girişimi önlemek için eklenen periyodik ön ekler çıkarılır. DFT bloğuna gönderilir ve buradan da paralel halde olan bit dizisi seri hale dönüştürülerek BPSK ile ters modülasyon işleminden sonra Turbo Kod Çözücü bloğuna verilir. OFDM alıcı kısmının çıkışında elde edilen sinyalin bölgesel dağılımı Şekil 10'da gösterilmiştir. Turbo Kod Çözücü çıkışında elde edilmiş kestirilmiş bit dizisi AES şifre çözme bloğuna verilir ve açık metin elde edilir. Sistemin genel blok yapısı Şekil 7'deki gibidir. Sistem modellemesi MATLAB 7.0 paket programı üzerinden gerçekleştirilmiştir.



Şekil 7. Sistemin Genel Blok Diyagramı

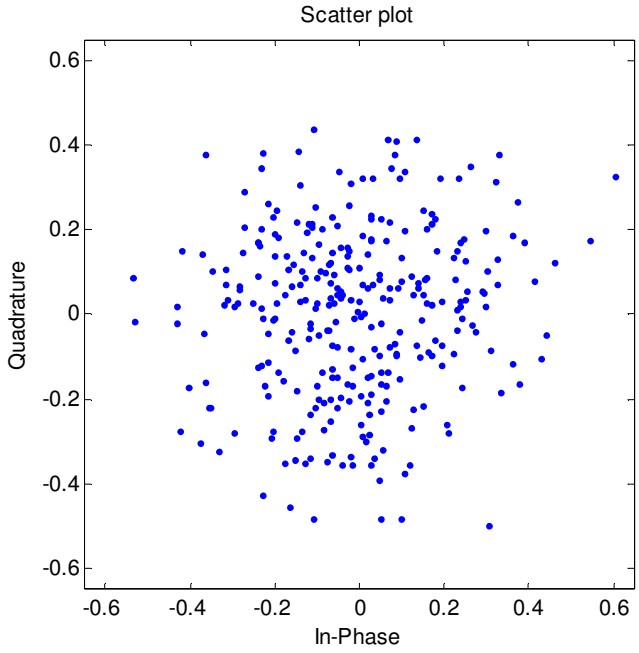
5.1. OFDM Verici Çıkışında Elde Edilen Sinyal Dağılımı



Şekil 8. OFDM Verici Çıkışındaki Sinyal Dağılımı

Sinyal, Turbo Kodlayıcı bloğundan geçtikten sonra OFDM verici bloğuna gönderilir. OFDM bloğunun çıkışında elde edilen sinyalin bölgesel dağılımı Şekil 8'deki gibidir.

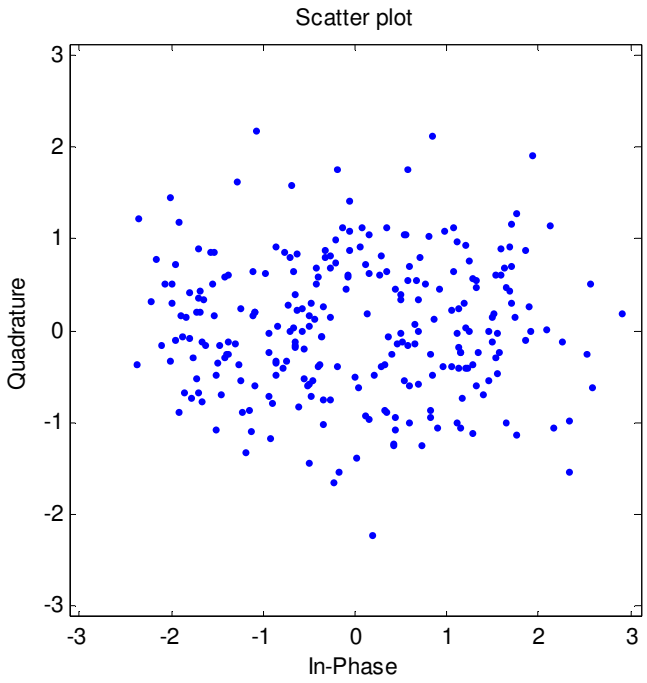
5.2. OFDM Verici Çıkışında Elde Ettiğimiz Sinyalin Üzerine AWGN Gürültü Eklediğimizde Elde Edilen Sinyal Dağılımı



Şekil 9. OFDM Verici Çıkışında Elde Ettiğimiz Sinyalin Üzerine AWGN Gürültü Eklediğimizde Elde Edilen Sinyal Dağılımı

Sinyal, OFDM verici bloğundan geçtikten sonra AWGN gürültüsü eklenmiş kanala gönderilir. Burada OFDM verici bloğunun çıkışında elde edilen sinyalin üzerine AWGN gürültüsü eklenir ve sinyal daha bulanık bir hal alır. Sinyalin, AWGN gürültüsü eklenmiş halinin bölgesel dağılımı Şekil 9'daki gibidir.

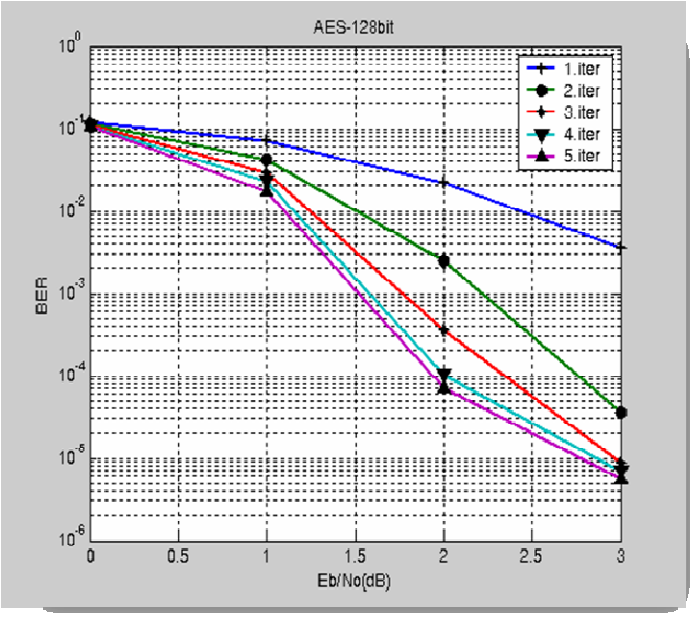
5.3. OFDM Alıcı Çıkışında Elde Edilen Sinyalin Dağılımı



Şekil 10. OFDM Alıcı Kısmında Elde Edilen Sinyalin Dağılımı

Sinyal, AWGN gürültüsü eklenmiş kanaldan geçtikten sonra OFDM alıcı bloğuna gelir. Şekil 10'da OFDM alıcı bloğunun çıkışında elde edilen sinyalin bölgesel dağılımı gösterilmiştir.

5.4. AES-TURBO Bloğu Kullanılarak Elde Edilen Performans Eğrisi

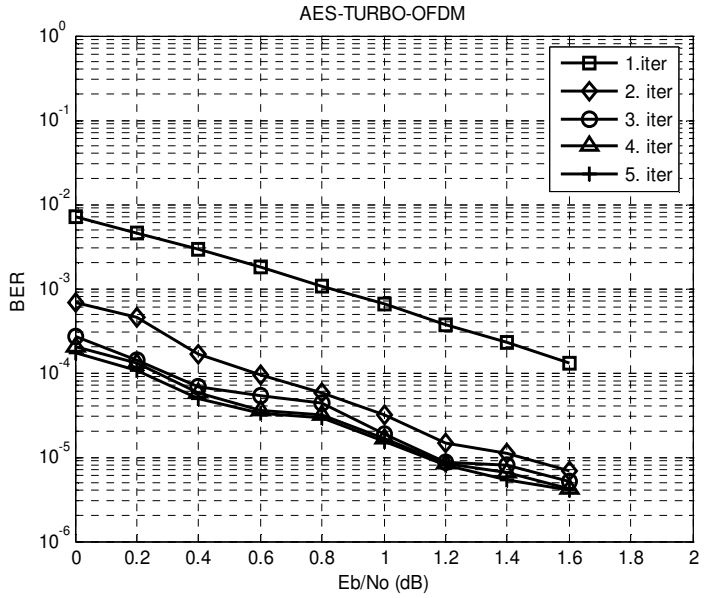


Şekil 11. AES-TURBO Sistemin Performans Eğrisi

Şekil 11'de AES şifreleme tekniği ile şifrelenmiş Turbo Kodlayıcı ile kodlanmış sistem ile elde edilen Sinyal Gürültü Oranının, Bit Hata Oranına karşılık gelen performans eğrileri gösterilmiştir. Elde edilen eğriye göre Shannon'un Bit Hata Oranı teorik limit değeri olan 10^{-5} seviyelerine inilmesi beklenilmiştir. Bu durumu pratik olarak şu şekilde açıklayabiliriz. Bir haberleşme sisteminde verici kısmından göndermiş olduğumuz 100.000 çerçeve'ye karşılık olarak alıcı kısmının çıkışında elde edilen 100.000 çerçeve içerisinden 1 çerçeve'de bozulma olması beklenilmektedir. Bu bilgiler ışığında Şekil 11'deki grafiği tekrar yorumlarsak Bit Hata Oranı değerinin 10^{-5} seviyesine inmesi için Sinyal Gürültü Oranı (SNR) değerinin 3 dB seviyelerinde olması gerekmektedir. Grafik üzerinde belirtilen iterasyon değerleri alıcı kısmında bulunan Şekil 4'te gösterilen Kod Çözücüden elde edilen değerlere göre çizdirilmiştir. 1. iterasyon değeri ile 5. iterasyon değeri arasında görülen bu farklılık tamamen kod çözücünün 5. iterasyon değerine doğru daha gerçek soft çıkışlar üretmesinden kaynaklanmaktadır. Örnek olarak

2. iterasyon değerini elde etmek için kod çözücü, sadece kanaldan alınan bilgileri değil, ilk iterasyonda ikinci Kod Çözücünün ürettiği giriş bitleri hakkındaki ek bilgiyi de kullanır. Bu fazladan bilgi, 1. kod çözücü bileşeninin daha gerçek soft çıkışlar oluşturmasını sağlar. Daha sonra bu çıkışlar da ikinci kod çözücü tarafından önsel bilgi olarak kullanılır. Bu döngü bu şekilde devam eder ve her iterasyonda kodu çözülen bitlerin Bit Hata Oranı değeri gitgide düşer.

5.5. AES-TURBO-OFDM Bloğu Kullanılarak Elde Edilen Performans Eğrisi



Şekil 12. AES-TURBO Kodlu OFDM Sisteminin Performans Eğrisi

Şekil 12'de AES şifreleme tekniği ile şifrelenmiş Turbo Kodlayıcı ile kodlanmış sisteme OFDM bloğu ekleyerek elde edilen performans eğrisine yer verilmiştir. Burada, AES-TURBO sisteminden farklı olarak Shannon'un teorik limit değeri olan 10^{-5} Bit Hata Oranı (BER) seviyelerine inmek için Sinyal Gürültü Oranı (SNR) değerinin 0,40-0,60 dB değerlerinde olması yeterli olduğu gözlemlenmiştir.

6. SONUÇ

Beyaz Gauss Gürültüsü eklenmiş (AWGN) kanal modelinde, AES-TURBO sisteminden elde edilen başarım eğrileri ile AES-TURBO-OFDM sisteminden elde edilen başarım eğrilerini karşılaştırdığımızda OFDM'in sisteminin performansına olan etkisi açıkça görülmektedir. AES-TURBO sistemde elde edilen başarım eğrilerinde Shannon'un limit değeri olan 10^{-5} Bit Hata Oranı (BER) seviyelerine inmek için Sinyal Gürültü Oranı (SNR) değerinin 3 dB değerlerinde olması gerekiyor. Fakat bu sisteme OFDM dahil olduğu zaman ise Shannon'un teorik limit değeri olan 10^{-5} Bit Hata Oranı seviyelerine inmek için Sinyal Gürültü Oranı (SNR) değerinin 0,40-0,60 dB aralığında olması yeterlidir.

Sonuç olarak AES ile şifrelenmiş Turbo Kodlayıcı ile kodlanmış OFDM sistemi, AES ile şifrelenmiş ve Turbo Kodlayıcı ile kodlanmış sisteme göre daha düşük SNR değerleri ile daha güvenilir haberleşme yapmak mümkündür.

TEŞEKKÜR
Bu çalışma sırasında değerli katkılarını ve yorumlarını esirgemeyen, İstanbul Üniversitesi Mühendislik Fakültesi değerli Öğretim Üyelerinden Prof. Dr. Hakan Ali ÇIRPAN ve Araş.Gör. Bahattin KARAKAYA'ya desteklerinden dolayı teşekkürü bir borç biliriz.

7. KAYNAKÇA

Daemen J. , Rıjmen V., (1999), "AES Proposal: Rijndael AES Algorithm Submission".

Özduran V., (2008),"Birleşik Şifreleme ve Turbo Kodlama Sistemleri", Yüksek Lisans Tezi, İstanbul Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

Özduran V., Uçan N.O., Gürel M., O. Osman, (2008), "Birleşik Şifreleme ve Turbo Kodlama Sistemleri", 2. Haberleşme Teknolojileri ve Uygulamaları Sempozyumu (HABTEKUS), Yıldız Teknik Üniversitesi, İstanbul.

Mahmood A., (2008), "Method to Improve Channel Coding Using Cryptography", World Academy of Science, Engineering and Technology 41.

Arnone L., Gonzalez C., Gayoso C., Moreıra Castıneıra J., Lıberatorı M., (2009), "Security and Ber Performance Trade-off in Wireless Communication Systems Applications", Latin American Applied Research, 39:187-192.

Çam H., Uçan N. O., Odabaşıoğlu N., Sönmez C. A., (2010) "Performance of Joint Multilevel/ AES-LDPCC-CPFSK Schemes Over Wireless Sensor Networks" International Journal Of Communication Systems, Volume:23 , Issue: 1, sf: 77-90.

Fıps 197, (2001), Advanced Encryption Standard, Federal Information Processing Standard (FIPS), Publication 197, National Bureau of Standards, U.S. Department of Commerce, Washington D.C.

Sakallı M. T., (2006), "Modern Şifreleme Yöntemlerinin Gücünün İncelenmesi", Doktora Tezi, Trakya Üniversitesi, Edirne.

Berrou C., Glavıeux A., Thıtımajshıma P., (1993), " Near Shannon Limit Error-Correcting Coding and Decoding: Turbo Codes", in ICC'93, Geneva, Switzerland, May 1993, sf.: 1064-1070.

C.E. Shannon, (1948), "A mathematical Theory of Communication", *Bell Sys. Tech. J.*, Vol: 27, sf. 379-423 ve 623-656.

Osman, O., Uçan, O. N., (2006), "Haberleşme Teorisi ve Mühendislik Uygulamaları", Nobel, İstanbul, ISBN 9944-77-039-6.

Osman, O., Uçan,O. N., (2003), "Bilgisayar Ağları Ve Haberleşme Teknikleri", İstanbul Üniversitesi, Isbn 975-404-695-6.

Osman, O., 2004, "Turbo Kodlama Tekniklerinin Başarımı", Doktora Tezi, İstanbul Üniversitesi,Fen Bilimleri Enstitüsü, İstanbul.

Van Nee R., Prasad R., (2000), "Ofdm For Wireless Multimedia Communications", Artech House Boston London, Isbn 1-58053-796-0.

Heıskala, J.,Terry, J., (2001), "Ofdm Wireless Lans: A Theoretical And Practical Guide", Sams Publishing, Usa, Isbn 0-672-32157-2.

İmamoğlu E.Seza, Taşpınar N., (2004), "Ofdm Sistemlerinde Tepe Gücü /Ortalama Güç Oranının Seçici Eşleme Tekniği Kullanılarak Azaltılması" Ursı-Türkiye'2004 Bilimsel Kongresi,Ulusal Genel Kurul Toplantısı,Bilkent Üniversitesi,Ankara, Sf:164-166.

Koraltürk, E., (2008), "Güç İletim Hatlarında Ortagonal Frekans Bölmeli Çoğullama ile Başarı Analizi" , Yüksek Lisans Tezi, İstanbul Üniversitesi, İstanbul.

Lıtwın L., Pugel M., (2001), "The Principles of Ofdm", *Rf Design*, Rf Signal Processing, Sf: 30-48.

Engels M., (2002), "Wireless Ofdm Systems: How To Make Them Work?", Kluwer Academic Publisher,Usa, Isbn 1-4020-7116-7.