Sinyal Karıştırıcıların LTE/LTE-A Aşağı-Hat Fiziksel Kanalına Etkileri

Gizay KISA [1] Özgür ERTUĞ [2]

[1,2] Elektrik Elektronik Mühendisliği Bölümü, Gazi Üniversitesi, Ankara
[1] e-posta: gizay.kisa@gazi.edu.tr [2] e-posta: ertug@gazi.edu.tr

Özetçe

Mobil teknolojilerdeki hızlı gelişmeler, kullanıcıların her geçen gün daha fazla veri kullanmasına olanak sağladı. Böylelikle daha geniş kapsama alanına, bant genişliğine, yüksek veri hızı ve kalitesi gibi gereksinimlere sahip mobil ağ standartları gelişti. Mobil ağ haberleşmesinin son sürümü olan LTE-A (Long Term Evolution-Advanced) bu standartları karşılamak üzere ortaya çıkarılmıştır. Ülkemizde 4.5G olarak da adlandırılın bu hizmet akıllı telefonlarımız aracılığıyla haberleşmenin yanı sıra doğal afetlerde, acil durum mesajı yayınlarında ve askeri amaçlı haberleşme sistemlerinde dahi kullanılabilmektedir. Fakat pek çok kablosuz iletişimde olduğu gibi LTE sinyallerinin de karıştırılması ve engellenmesi mümkündür. Bu çalışmada sivil uygulamalar için tasarlanan bu standardın, aşağı-hat (DL) fiziksel kanalına Baraj (Barrage), Kısmi Bant (Partial Band), Tek Tonlu (Single Tone) ve Çok Tonlu (Multitone) sinyal bozucu etkileri incelenerek, LTE/LTE-A sisteminin sinyal karıştırıcılara karşı Bit Hata Oranı(BER)-Sinyal Gürültü Oranı(SNR) enerji verimliği hesaplanacaktır.

Abstract

Swift advances in mobile technology have lately made it possible for users to utilize more and more data. As a result, mobile network standards with requirements such as wider coverage and band width, high data rate and quality have developed. LTE-A (Long Term Evolution-Advanced) as the final version of mobile network communication has been introduced with a view to coming up to the said standards. This service named as "4.5G" in our country can be utilized in state-of-emergency message broadcasts and military communication systems as well as communications via smart phones. However, LTE signals can be intercepted or jammed, which is the case for all wireless communication systems as well. In this study, energy efficiency of LTE/LTE-A concerning Bit Error Rate (BER) and Signal-to-Noise Ratio (SNR) against signal jammers will be figured out by examining beforehand the signal jamming effects of this standard designed for civil practices on downlink channel, namely barrage, partial band, single tone and multitone jammer.

I. Giriş

3GPP tarafından uzun yıllar süren standartlaşma çalışmalarından sonra ilk LTE kavramı hayatımıza Sürüm 8 adıyla 2008 yılında girmiştir. Bu sürüm daha önceki sistemlere kıyasla önemli ölçüde gelişmiş veri performansı sağlayan tamamen yeni bir radyo ara yüzü ve çekirdek ağı içermektedir. Bir yıl sonra, Sürüm 9 adıyla yeni bir standart yayınlanmıştır. Sürüm 9, Sürüm 8'de sunulan özelliklerin yanı sıra yeni bir ağ mimarisi ve servis özellikleri sağlamaktadır. 2011 yılın da ise LTE-A yani 4.5G'nin başlangıcı olduğu düşünülen Sürüm 10 ile veri aktarımı geliştirilmiş ve hücre kapsama alanı önemli ölçüde genişletilmiştir.

LTE-A tartışmasız bir şekilde en iyi hücresel standart olma yolundadır. Küresel Mobil Tedarikçiler Birliği (Global Mobile Suppliers Association) birliği tarafından Ağustos 2016 yılındaki verilere göre LTE/LTE-A şimdiden 170 ülkeden 521 operatör ile ticari olarak kullanıma sunulmuştur [1]. Aynı zamanda ABD'de kamu güvenliği alanında, doğal afetler ve kriz durumlarında yayın (broadcast) mesajı iletmek için FirstNet adıyla bir LTE standardı kullanılmaktadır [2]. LTE'nin diğer bir kullanım alanı da askeri amaçlıdır. ABD ordusu savaş alanında iletişimi sağlamak, video, ses ve veri de dâhil olmak gerekli görev parametrelerini aktarmak ve uçak gemileriyle uçaklar arasındaki haberleşmeyi sağlamak için LTE kullanmaktadır [3]. Bu sebeple kritik alanlarda da kullanımı artan ve büyük bir potansiyele sahip olan LTE-A standardının güvenilirliği oldukça önemli bir konudur.

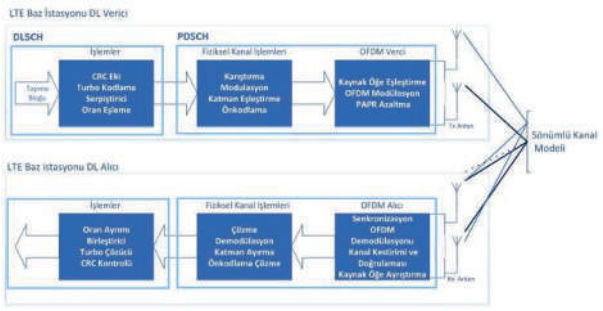
Literatürde radar ve telsiz sinyali için karıştırıcı saldırılar geniş bir biçimde incelenmiş olmasına rağmen haberleşmedeki sinyal karıştırma saldırılarıyla ilgili daha az çalışma yapılmıştır. LTE'ye yönelik tehditler, algılama yöntemleriyle ilgili en genel çalışma [4]'da sunulmuştur. Bir başka çalışma olan [5, 6] baraj sinyal karıştırıcıdan yola çıkarak saldırılara müsait LTE/LTE-A fiziksel kanalları ve sinyallerini belirlemiştir. [7]'de alt sistemden ana sisteme yukarı-hat (uplink), aşağı-hat haberleşmeye ve baz istasyonlarına karşı olan akıllı sinyal karıştırıcı saldırılarına karşı tehditleri inceleyerek teorik çözüm önerileri sunmuştur. [8]' de akıllı dar bant sinyal karıştırıcısı kullanılarak şebeke çapında yapılan Hizmet Reddi (DDoS) saldırısıyla ilgili çalışma yapmıştır.

LTE standardına yönelik saldırıları Hizmet Reddi Saldırıları (DDoS) ve bilgi ayıklama olarak ikiye ayrılmaktadır [9]. Sinyal bozma saldırıları genelde hizmet reddi saldırılarına sebep olurken siber saldırılarda bilgi ayıklamaya yönelik saldırılardır. Bu çalışmada diğer hizmet reddi saldırılarına sebep olan sinyal bozucu çalışmalarından farklı olarak sadece fiziksel kanaldaki aşağı-hat haberleşme çalışılmış olup, [6, 10 ve 11]' da belirtilen baraj, kısmi bant, tek-tonlu ve çok-tonlu sinyal karıştırıcılar kullanılarak (Sinyal-Gürültü Oranı) SNR 'a karşı (Bit Hata Oranı) BER performansları gerçekleştirilmiştir. Makalenin II. bölümünde LTE standardının aşağı-hat fiziksel katmanı hakkında, III. bölümünde ise LTE/LTE-A'e yönelik saldırılarda kullanılan sinyal karıştırıcıları hakkında kısa bilgiler verilmiştir. Son olarak IV. bölümünde ise simülasyon

neticesinde ortaya çıkan sonuçlar grafikleri ile birlikte gösterilmektedir.

II. LTE Aşağı-Hat Fiziksel Katmanı

LTE fiziksel katmanı, gelişmiş bir baz istasyonu (eNodeB) ile mobil kullanıcı ekipmanı (UE) arasında hem veri hem de kontrol bilgisini iletmek için oldukça etkili bir katmandır. Bu katman üst katmanlardan aktarılan veri bitleri üzerinde yapılan tüm işlemleri içermektedir. Hücresel uygulamalar için yeni geliştirilmiş şebeke bütünleştirmesi (carrier aggregation), dikgen frekans-bölmeli çoğullama (orthogonal frequency division multiplexing), turbo kanal kodlama (turbo coding), kanal denkleştirici (channel equalizer), kanal kestirimi (channel estimation), çoklu giriş ve çıkış (MIMO) yöntemleri bu katmanda kullanılmaktadır.



Şekil 1 LTE aşağı-hat fiziksel katmandaki alıcı ve verici yapısı

Şekil 1'de aşağı-hat fiziksel katmandaki alıcı ve verici yapısı gösterilmiştir. Fiziksel katman işlemleri DL Paylaşılan kanalı (DLSCH) ve Fiziksel DL Paylaşılan Kanalı (PDSCH) olmak üzere iki basamaktır. Fiziksel katmanda verici işlemi taşıma blokları şeklinde gruplanmış kaynak veri bitleri ile başlar. Taşıma bloklarındaki hata tespitleri için Periyodik Artıklık Denetimi (CRC) kullanılır. Bunu da transport bloğu sonuna CRC Eşlik Bitleri (parity bits) ekleyerek sağlar. Ardından en güçlü kanal kodlama yöntemlerinden biri olarak kabul edilen turbo kanal kodlama yöntemi kullanılır. Turbo kodlama da veri bloklarına Artık Bit (redundant bit) ilave ederek kanal kapasitesini geliştiren İleri Hata Düzeltme (FEC) yöntemidir. Bu yöntem içerisinde evrişimli kod (convolutional code) un yanında karıştırıcılar (interleaver) kullanılmaktadır. Böylelikle spektral çeşitlilik sağlanabilmektedir. Oran eşleştirme bloğu ile istenen kod oranıyla iletilecek veri akışı oluşturulmaktadır. Oluşturulan her bir kodlu kelime (codeword) dikey bir dizi ile çarpılarak karışık bir semboller dizisi oluşturulur. Ardından karıştırılmış şifreli kod sözcükleri QPSK, 16 QAM ve 64 QAM modülasyonlarından birine uğrayarak karmaşık sembollere dönüştürülmektedir. Katman haritalandırma (layer mapping) ve önkodlama (precoding) blokları MIMO haberleşme için gerekli olan iki aşamadır. Çeşitliliği arttırmak için kullanılan birleştirici metodları bu katmanda uygulanmaktadır. Bu sayede uzamsal çoklama (spatial multiplexing), verici çeşitliliği (transmit diversity) ve tek anten ile iletişim (single antenna port transmission) gibi seçenekler kullanılır. Verici zincirindeki son adımda ise dik frekans bölmeli çoğullama (OFDM) uygulanmaktadır. Bu yöntem ile her bir sembol birbirine dik alt taşıyıcılara bindirilmektedir. Böylelikle spektral verimlilik sağlanmaktadır. Sistemin alıcı tarafında ise bu blok yapılarına ilaveten kanal denkleştirici ve kanal kestirimi aşamaları yer almaktadır. Kanal kestirimi ile kanalın frekans tepkisi (frequency response) tahmin edilmektedir. Böylelikle kanal denkleştirici, tahmin edilen kanalın frekans tepkisini kullanarak frekans ekseninde eşleştirme işlemi yapmaktadır.

III. Sinyal Bozucuların LTE Fiziksel Katmanına Etkisi

LTE/LTE-A bağlantısı "fiziksel kanallar" ve "fiziksel sinyaller "den oluşur. Bu fiziksel kanallar ve sinyaller, zaman ve frekansta birleştirilerek ve zaman-frekans çerçevesi üzerinde eşlenir. LTE çerçevesindeki fiziksel kanalların haritalandırılması ise her ana istasyon tarafından gönderilen yayın (broadcast) mesajlarıyla tanımlanır. Bu haritalama yöntemi esnasında sinyal bozucular, belirli kaynak elemanlarını da (resource elements) bulunan verileri bozabilir veya belirli kanal ve sinyalleri engelleyebilirler. Bu çalışmada kullanılan bozucu yöntemleri baraj sinyal karıştırıcı, kısmi bant sinyal karıştırıcı, tek tonlu sinyal karıştırıcı ve çok tonlu sinyal karıştırıcı olarak sıralanmaktadır.

A. Baraj Sinyal Karıştırıcı (BJ)

Baraj sinyal karıştırıcı hedef sinyal hakkında ek bilgi gerektirmediği için en basit saldırı yöntemi olarak kabul edilmektedir. Bu metotta tüm banda Toplanır Beyaz Gauss Gürültü (AWGN) bindirilerek gürültü seviyesi arttırılır. Böylece hedefin aldığı Sinyal-Gürültü Oranı (SNR) düşer. Baraj sinyal karıştırıcı çok etkili bir yöntem olmasına karşın çok fazla güç gerektirmektedir [12].

B. Kısmi Bant Sinyal Karıştırıcı (PBJ)

Kısmi bant karıştırıcıda, baraj sinyal karıştırıcıdan farklı olarak LTE sisteminin bant genişliğinin sadece belirli bir bölümü hedeflenir. Hedeflenen bant genişliğine yine sabit bir AWGN bindirilerek gürültü seviyesi artırılır. Özelikle LTE'de senkronizasyon sinyallerini karıştırmak için kısmi bant sinyal karıştırıcı kullanılabilir. [13]

C. Tek Tonlu Sinyal Karıştırıcı (STJ)

Tek tonlu sinyal karıştırıcı, kısmi bant karıştırıcısının bir çeşidi olarak sınıflandırılabilir. Her tek ton, LTE standardındaki tek bir alt taşıyıcıyı karıştırmak için kullanılır. Bu ton genellikle darbe, dikdörtgen ve AWGN şeklinde olabilmektedir. Tek tonlu sinyal karıştırıcı alt taşıyıcıyı karıştırabilmek için tek bir tonu yüksek güçte iletir. Tek tonlu sinyal karıştırıcı Denklem 1'de gösterilmektedir.

$$J(t) = A_j \cos(2\pi f_j t) = \sqrt{2J}\cos(2\pi f_j t) \qquad (1)$$

A_j Sinyal karıştırıcının genliği, J gücü ve f_j tonun merkez frekansıdır. Tek tonlu sinyal karıştırıcı için hedef sistemin taşıyıcı frekans bilgisi gerekmektedir [13]. Genellikle hedefin Otomatik Kazanç Kontrol mekanizmasını bozmak için kullanılır ve bu sayede dolaylı olarak alt-taşıyıcıları karıştırmaktadır [10].

D. Çok tonlu Sinyal Karıştırıcı (MTJ)

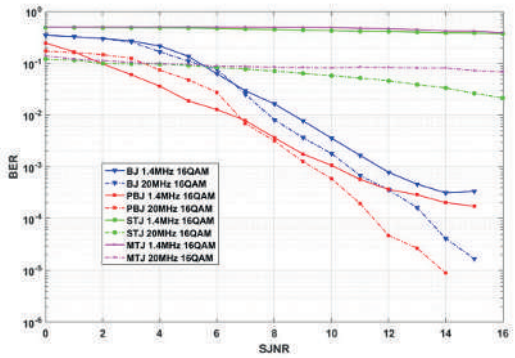
Çok tonlu Sinyal Karıştırıcı, tek tonlu sinyal karıştırıcıdan farklı olarak birden çok alt-taşıyıcıyı karıştırmak için eşit güçte ve çok sayıda ton üretir. Özellikle iletilen sinyal karıştırıcının gücü sınırlı olduğunda, iletilen tonların sayısı arttırılarak sinyal karıştırıcının gücü düşürülür. Her bir ton, Denklem 2'de ifade edilmiştir.

$$J(t) = A_j \sum_{k=1}^{N_T} \cos(2\pi f_k t) = \sqrt{\frac{2J_T}{N_T}} \sum_{k=1}^{N_T} \cos(2\pi f_k t) \quad (2)$$

Burada A_j sinyal karıştırıcının genliğini, J_T gücü ve f_k k^{th} alt-tonların merkez frekanslarını ifade etmektedir [14].

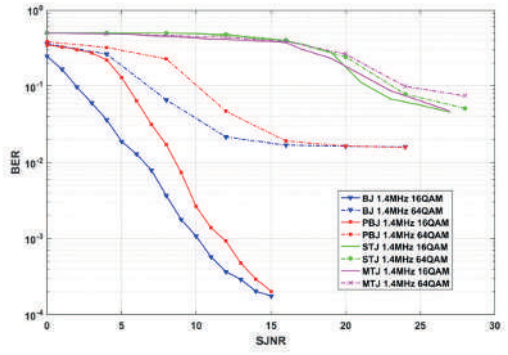
IV. Simülasyon Sonuçları ve Analizler

Bu kısımda, oluşturulan LTE/LTE-A DL fiziksel katmanın BJ, PBJ, STJ ve MTJ sinyal bozucu etkileri karşısında, bant genişliği ve modülasyon seviyelerine göre BER- SJNR performansı gösterilmiştir. Kanal yapısı olarak frekans seçici sönümlemeli şehir içi kanal tercih edilmiştir. Simülasyon parametreleri sırasıyla: Alıcı anten sayısı 1, verici anten sayısı 1, kanal bant genişliği 1.4 MHz ve 20 MHz, modülasyon tipi 16 QAM ve 64 QAM, OFDM için 1.4 MHz ve 20 MHz bant genişliğinde sırasında FFT genişliği 128 ve 2048, kodlama oranı 1/3, maksimum turbo şifre çözme döngü sayısı 6, taşıyıcı frekans 2.5 GHz olarak seçilmiştir. Tüm simülasyonlarda Monte Carlo simülasyon metodu kullanılmıştır. BER performansları çıkartılırken maksimum hata sayısı ve maksimum bit sayısı bir milyondur.



Şekil 2 Sinyal bozucuların 1.4 MHz ve 20MHz bant genişlikleri BER- SJNR performansı

Şekil 2 'de tüm sinyal bozucuların 1.4 MHz ve 20 MHz bant genişliklerinde ve 16 QAM modülasyon tekniği altında bozucu etkileri test edilmiştir. Üç farklı karıştırıcıya 10 dB SJNR ve 20 MHz değerinde bakıldığında, LTE DL fiziksel kanalı sırasıyla BJ'de $1.8\text{x}10^{-3}$, PBJ'de $5.8\text{x}10^{-4}$, STJ'de 0.058 ve MTJ'de ise 0.0817 bit hata oranına sahiptir. Benzer şekilde 10 dB SJNR ve 1.4 MHz değerinde bakıldığında, BJ'de $3.59\text{x}10^{-3}$, PBJ'de $1.072\text{x}10^{-3}$, STJ'de 0.4287 ve MTJ'de ise 0.4907 bit hata oranına sahiptir. Buna göre, her iki bant genişliğinde de MTJ'nin bozucu etkisinin en fazla olduğu, sırasıyla da STJ, BJ ve PBJ'nin geldiği gözlemlenmektedir. Aynı zaman da 10^{-3} bit hata oranında 1.4 MHz ve 20 MHz bant genişlikleri arasında BJ'nin 1.1dB, PBJ'ın ise 0.8dB'lik bir enerji farkının olduğu gözlemlenmiştir. Bu verilerden yola çıkarak 20 Mhz'lik bant genişliğinde daha az enerjiyle 1.4 MHz'lik bir sistemdeki bit hata oranına sahip olunabildiği görülmektedir.



Şekil 3 Sinyal Bozucuların 16 QAM ve 64 QAM Modülasyonlarında BER- SJNR performansı

Şekil 3'de 1.4 MHz bant genişliğinde 16 QAM ve 64 QAM modülasyon uygulandığında BJ, PBJ, STJ ve MTJ'ın bozucu etkileri incelenmektedir. 10 dB SJNR değerinde modülasyon teknikleri karşılaştırıldığında, 16 QAM modülasyonunda BJ'nin $1.072\text{x}10^{-3}$, PBJ $2.63\text{x}10^{-3}$, STJ 0.4907 ve MTJ ise 0.4287 BER değerlerine sahip iken, 64 QAM modülasyonda BJ $3.162\text{x}10^{-2}$, PBJ $1.13\text{x}10^{-1}$, STJ 0.47 ve MTJ 0.49 BER değerlerine sahiptir. 16 QAM modülasyon tekniğinde tüm kanal bozucuların etkisinin en az olduğu görülmüştür. Bunun nedeni ise 16 QAM modülasyon tekniğinde yıldız kümesi diyagramında (constellation diagram) her bir sembolleri arası mesafenin 64 QAM modülasyona göre daha geniş olmasıdır. Şekil 3'te görüldüğü üzere 15 dB SJNR ve 20 dB SJNR değerinden sonra BJ ve PBJ uygulandığında 64 ve 16 QAM modülasyon BER performansları yakınsamaktadır. Sonuç olarak bu değerlerden sonra sinyal gücü arttırılsa bile enerji verimliliği değişmemektedir. Ayrıca STJ ve MTJ kanal bozucu teknikleri arasında ise 21dB SJNR değerinden sonra 16QAM ve 64QAM modülasyon teknikleri için 10^{-1} BER değerinde yaklaşık 1dB'lik enerji farkı oluşmaktadır.

V. Sonuç

Bu çalışmada BJ, PBJ, STJ ve MTJ kanal bozucuların LTE/LTE-A DL fiziksel kanalına etkileri incelenmiştir. MTJ'nin sırasıyla STJ, BJ ve PBJ'ye göre daha bozucu etkisi olduğu gözlemlenmiştir. Ardından her bir kanal bozucunun farklı modülasyon türlerindeki bozucu özellikleri gözlemlenmiştir. Bunun için kullanılan modülasyon türleri LTE/LTE-A DL standardında yer alan 16 QAM ve 64 QAM modülasyon tekniklerdir. 16 QAM modülasyonun tüm kanal bozucular altında daha dayanıklı olduğu gözlemlenmiştir. İncelenen ikinci bir özellik ise LTE sistemlerinde kullanılan en düşük ve en yüksek bant genişliklerinin kanal bozuculara karşı etkisi gözlemlenmiş, 20 MHz'lik bant genişliği kullanımında kanal bozucuların etkisinin daha az olduğu görülmüştür.

VI. Kaynakça

[1] GSA, (2016). GSA confirms 521 LTE networks launched, LTE-Advanced now mainstream. [Web] https://gsacom.com/press-release/gsa-confirms-521-lte-networks-launched-lte-advanced-now-mainstream/ [ET: 26 Mayıs 2017].

[2] Kruger, L, (2017). The First Responder Network (FirstNet) and Next - Generation Communications for Public Safety: Issues for Congress. Congressional Research Service.

[3] E. Thompson, (2012). Army examines feasibility of integrating 4G LTE with tactical network. RDECOM CERDEC Public Affairs. [web]. Available: http: //www.army.mil/article/87875/

[4] R. Jover, (2013). Security attacks against the availability of lte mobility networks: Overview and research directions.*Wireless Personal Multimedia Communications (WPMC), 2013* 16th International Symposium .

[5] Lichtman, M., Jover, R., Labib, M., Rao, R., Marojevic, V. and Reed, J. (2016). LTE/LTE-A jamming, spoofing, and sniffing: threat assessment and mitigation. *IEEE Communications Magazine*, (54).

[6] M. Lichtman et al. (2016). A communications jamming taxonomy. *IEEE Security & Privacy*, vol. 14, no. 1.

[7] Jover, R., Lackey, J. and Raghavan, A. (2014). Enhancing the security of LTE networks against jamming attacks. *EURASIP Journal on Information Security*.

[8] F. M. Aziz, J. S. Shamma and G. L. Stüber. (2014). Resilience of LTE networks against smart jamming attacks. *IEEE Global Communications Conference*, Austin, TX.

[9] M. Lichtman, J. H. Reed, T. C. Clancy, and M. Norton. (2013). *Vulnerability of LTE to Hostile Interference.*

[10] Shahriar et al. (2015). PHY-Layer Resiliency in OFDM Communications: A Tutorial. *IEEE Communications Surveys & Tutorials,* vol. 17, no. 1, s. 292-314.

[11] Rohde& Schwarz. (2014). Vulnerabilities of LTE and LTEAdvanced Communication. *White Paper*.

[12] T. Basar. (1983). The Gaussian test channel with an intelligent jammer. *IEEE Trans. Inf. Theory,* vol. IT-29, no. 1, s. 152–157

[13] J. Luo, J. Andrian, and C. Zhou. (2007). Bit error rate analysis of jamming for OFDM systems. *Wireless Telecommunications Symposium*.

[14] S. Chao, W. Ping, and S. Guozhong. (2012). Performance of OFDM in the presence of multitene jamming. *Proc. IEEE ISRA*, s. 118–121

[15] Zarrinkoub, H. (n.d.). *Understanding LTE with MATLAB*.