ÖZET

KABLOSUZ AĞLARDA MUTLAK GÜVENLİK VE KİMLİK DOĞRULAMASI SAĞLANMASI İÇİN OTOMATİK TEKRAR TALEP SİSTEMİ

İleri düzey kablosuz haberleşme sistemleri için gizli dinlemelere karşı güvenlik ve kimlik taklidi (spoofing) ataklarına karşı kimlik doğrulaması sağlanmasına yönelik güvenli bir sistem ve yöntem açıklanmaktadır. Yöntem, gizliliğin elde edilmesi için maksimal oran birleştirmesi (MRC) yardımıyla birlikte, MAC katman mekanizması olarak otomatik tekrar talebi (ARQ) ve fiziksel katman (PHY) mekanizması olarak yapay gürültüden (AN) faydalanmaktadır. Temel olarak kanal içerisinde sınıf uzay gerektirmeyen özel bir yapay gürültü, hizmet kalitesi (QoS) gereklilikleri ve meşru taraflar arasındaki kanal koşulu esas alınarak tasarlanır ve veri paketine eklenir. Meşru alıcı (Bob) tarafından aynı paketin talep edilmesi durumunda, bir yapay gürültü iptal sinyali uygun şekilde tasarlanarak bir sonraki pakete eklenir. Ardından, Bon tarafından MRC süreci kullanılarak yapay gürültü bulunmayan bir paket elde edilir ve bu sırada gizli dinleme yapan tarafın performansı yapay gürültü tarafından bozulur.

İSTEMLER

1. Buluş, kablosuz haberleşme sistemlerinde alıcı tarafta ekstra değişiklikler yapılmadan ya da ekstra değişikliklere yol açılmadan ve gizli anahtarlar kullanılmadan ya da paylaşılmadan gizli dinlemelere karşı mutlak veri gizliliği ve spoofing'e karşı veri kimliği doğrulaması sağlamak üzere tasarlanan, paşağıdakilerden oluşan, bir yöntem ve sistem içermesi karakterize edilir:

- Verici üzerinde Tx çalışan ve cihaz içerisinde transfer edilmesi gerekli veri paketlerini güvenli, saklı veri paketlerine dönüştürebilen, ARQ birinci turunda iletilecek veri paketine eklenen, sıralı gürültü r1 adında, en az bir adet üst üste binen superimposed karıştırıcı sinyal;
- Verici üzerinde Tx çalışan ve cihaz içerisinde transfer edilmesi gerekli veri paketlerini güvenli, saklı veri paketlerine dönüştürebilen, ARQ ikinci turunda iletilecek veri paketine eklenen, sıralı gürültü r2 adında, en az ikinci bir üst üste binen superimposed karıştırıcı sinyal;
- Veri alım kalitesi güvenilirliği iyileştirilirken, üst üste binmiş superimposed karıştırıcı sinyallerin r1 ve r2 girişim etkisini iptal etmek ve kaldırmak üzere, birinci alınan veri paketini ve ikinci alınan veri paketini tasarlanmış bir şekilde birleştirebilecek, en az bir maksimal oran kombinasyonu (MRC) süreci.

2. İstem 1'e göre, kablosuz ağlarla güvenli veri alışverişi yapabilecek bir cihaz üzerindeki verici Tx üzerinde çalışabilecek şekilde yapılandırılan, meşru kanal genişliği ile güvenlik altına alınacak hizmetin QoS gerekliliklerinin bir fonksiyonu olmak üzere uygun şekilde tasarlanan, üst üste binen superimposed karıştırıcı sinyallerin ve eklenmesiyle karakterize edilen bir sistemdir.

3. İstem 1' e göre, farklı bir pozisyonda bulunan alıcı düğümlerde girişime yol açarken, sadece meşru alıcının lokasyonundaki girişim etkilerini tamamen iptal edecek şekilde tasarlanan ve yapılandırılan üst üste binmiş superimposed karıştırıcı sinyallerin ve eklenmesiyle karakterize edilen bir sistemdir.

4. İstem 1'e göre, uzamsal serbestlik derecesinin (çoklu antenlerle oluşturulan sıfır uzayın) bulunmadığı, kanalın düz sönümleme içerisinde yer aldığı (yani daha fazla ihtimal olmaması) ve verici tarafta tek bir antenin bulunduğu en zorlu senaryolardan birinde gizliliği sağlayabilmesi ile karakterize edilir.

5. İstem 1'e göre, sadece gizliliğin arttırılması için değil aynı zamanda PAPR seviyesinin azaltılması ve OFDM tabanlı sistemlerin OOBE seviyesinin hafifletilmesi gibi gizliliğin yanı sıra diğer amaçlar için da faydalanılabilecek eklenen AN'den dolayı kuvvet alanı içerisinde ekstra serbestlik derecesi oluşturması ile karakterize edilir.

6. İstem 1'e göre, dağıtıcı kanallar üzerinden OFDM tabanlı dalga formlarıyla kullanıldığında elde edilebilmesi ile karakterize edilir.

TARİFNAME

KABLOSUZ AĞLARDA MUTLAK GÜVENLİK VE KİMLİK DOĞRULAMASI SAĞLANMASI İÇİN OTOMATİK TEKRAR TALEP SİSTEMİ

Teknik Alan

Bu buluş, ileri düzey kablosuz haberleşme sistemleri (5G ve üzeri sistemler gibi) için, eş zamanlı bir şekilde, gizli dinlemelere karşı gizlilik ve kimlik taklidi (spoofing) saldırılarına karşı kimlik doğrulama sağlayan güvenli bir yöntem ve sistemle ilgilidir.

Tekniğin Bilinen Durumu

Veri iletiminin gizli dinlemelere karşı korunması (gizlilik), geleneksel olarak, söz konusu anahtarların, bilinmesi ve tahmin edilmesi için çok geniş kapsamlı ve ayrıntılı araştırmalar gerçekleştirilmesi gerekliliğinden kaynaklanan aşırı karmaşıklıktan dolayı, gizlice dinleme yapmak isteyenler tarafından bilinemeyeceği ya da anlaşılamayacağı varsayımıyla, verici ve alıcı taraf arasında paylaşılan gizli anahtarların kullanılması suretiyle şifreleme ve şifre çözme işlemlerini gerçekleştiren şifreleme esaslı yöntemlerden faydalanılarak elde edilmiştir.

Ancak, şifreleme esaslı yöntemlerin, gelecekteki kablosuz haberleşme senaryoları içerisinde uygun bir şekilde kullanılmalarına olanak tanımayan, aşağıda gösterilen sakıncaları bulunmaktadır.Söz konusu sakıncalar, aşağıdaki şekilde özetlenebilecektir: Birincisi, meşru taraflar arasındaki anahtar oluşturma, dağıtım ve yönetim süreçleri, özellikle büyük ölçekli heterojen ve merkezi olmayan kablosuz ağlar içerisinde, aşırı derecede zorludur. İkincisi, anahtar uzunluğunun arttırılması, günümüz veri hacmi içerisinde Shannon'un mükemmel gizliliğine sahip güvenlik yöntemlerinin uygulanmasının pratik olmamasının yanı sıra, daha fazla kaynak kaybına yol açmaktadır. Üçüncüsü, bilgisayar ve bilgi işlem cihazlarındaki hızlı gelişmeler ve ilerlemeler, mevcut gizli anahtar esaslı tekniklerin, özellikle kuantum bilgisayarların hayata geçmesiyle birlikte, matematiksel açıdan ne kadar karmaşık olurlarsa olsunlar, çözülebileceği gerçeğini ortaya koymaktadır. Dördüncüsü,

şifreleme esaslı güvenlik, otonom sürüş, uzaktan ameliyat, insansız hava araçlarının (İHA) kontrol edilmesi vs. gibi dokunsal haberleşme uygulamalarında ekstra gecikmelere ve karmaşıklıklara yol açmaktadır. Bu uygulamalar için, en az gecikmeyle en yüksek seviyede güvenli haberleşme sağlanması gerekmektedir.

Yukarıda bahsedilen problemlerden dolayı, anahtarsız fiziksel (PHY) katman güvenliği, kablosuz iletimleri, gürültü, güç kaybı, parazit, dağılım ve çeşitlilik dahil olmak üzere kablosuz kanalın doğal özelliklerinden faydalanılarak gizli paylaşılmış anahtarlar kullanılmadan, gizli dinlemelere karşı korumak üzere kullanılabilecek, gelecek vaat eden ve köklü değişiklik getiren bir konsept olarak ortaya çıkmıştır.Bunun elde edilmesi, sadece verici taraf (Alice) ve alıcı taraf (Bob) arasındaki kanalın doğal olarak, Alice ile gizli dinleme yapan kişi (Eve) arasındaki kanaldan daha iyi olması durumunda mümkündür. Ancak bu koşul uygulamada, Eve'in, (Bod'dan çok Alice'e yakın olabilecek) lokasyonu ve kanal gerçekleştirme sürecinin meşru tarafların (Alice ve Bob) haberleşmesi açısından pasif durumda bulunmasından dolayı, verici tarafla ilgili olarak, Bob'dan daha iyi kanala sahip olabileceği, kablosuz haberleşme senaryolarında garanti edilememektedir.

Buluşun Çözümünü Amaçladığı Teknik Problemler

Tekniğin bilinen durumunda, yukarıdaki problemin (Eve'in kanalının Bob'dan daha iyi olması) çözümüne yönelik muhtelif PHY güvenlik yöntemleri teklif edilmiştir.Söz konusu yöntemlerin büyük bir çoğunluğu esas olarak, aşağıdaki yaklaşımlardan biri ya da daha fazlasından faydalanılmasına bağlıdır: 1) paylaşılan anahtarların çıkarılması için çeşitlilik yardımıyla kanal varyasyonları ve karşılıklılığı; 2) örneğin, AN eklenmesi (Yapay Gürültü), ön kodlama işlemlerinin gerçekleştirilmesi, anten örüntülerinin güvenilir kullanıcılara doğru şekillendirilmesi (huzme biçimlendirme) vs. için MIMO, röleler ve geniş ölçekli ağlar gibi uzam çeşitlemesi, 3) Eve'in veri almasının engellenmesi için periyodik ön ekler, pilotlar, donanım bozulmaları gibi belirli sistemler içerisinde spesifik özellikler. Ancak, bu serbestlik seviyelerinin temin edilememesi, PHY güvenliğinin elde edilmesi aşırı zor bir hal almaktadır. Bütün bu kısıtlamalara rağmen, MAC katmanında hizmet kalitesi (QoS) gerekliliklerivle

bağlantılı mevcut özelliklerden faydalanmak suretiyle güvenlik sağlanabilecektir. Güvenliğin arttırılması için, örneğin, sadece planlanan alıcıların yeniden iletimleri talep edebilmesinden faydalanan (ARQ/HARQ) protokolü kullanılabilecektir.

Bu açıklamada (buluş özeti), ses ve görüntü gibi muhtelif veri hizmetlerine yönelik güvenliğin arttırılması amacıyla, MRC alıcı yapısından faydalanan sıfır uzayından bağımsız Yapay Gürültü ile ARQ mekanizmasına dayanan yeni bir birleşik PHY/MAC güvenlik yöntemi geliştirilmiş ve bulunmuştur.Bundan dolayı, çoklu antenlerde, müşterek rölelerde, frekans seçici kanallarda, OFDM'deki periyodik ön ek özelliğinde ya da yapay gürültü oluşumu için tam çift yönlü hedef varış noktalarında mevcut serbestlik seviyesiyle oluşturulan sıfır uzaya güvenmek yerine, bu çalışmada, gizli dinleme saldırılarına karşı iletimin korunması için sıfır uzaydan bağımsız yapay gürültü üretimi için literatürde ilk defa MRC'li ARQ'den faydalanılmaktadır. Temel olarak yapay gürültü, hizmet kalitesi (QoS) gereklilikleri ve meşru taraflar arasındaki kanal koşulu esas alınarak tasarlanır ve veri paketine eklenir. Bob tarafından aynı paketin talep edilmesi durumunda, meşru kullanıcının kanalı esas alınarak bir yapay gürültü iptal edici sinyal tasarlanır ve bir sonraki pakete eklenir. Ardından, MRC süreci kullanılarak yapay gürültü bulunmayan bir paket elde edilir ve bu sırada gizli dinleme yapan tarafın performansı yapay gürültü tarafından bozulur.

Açıklanan buluşun faydaları aşağıdaki şekilde ifade edilebilir:

- Yapısal olarak basit olmakla birlikte çok etkindir ve karmaşık verici mimarisi tarafından desteklenmesine gerek bulunmamaktadır. Daha önemlisi, MRC süreci sırasında mükemmel bir şekilde iptal edilebilecek, eklenen yapay gürültünün uygun tasarımı sayesinde, alıcı tarafında herhangi bir değişiklik ya da ekstra işlemlerin yapılmasına gerek bulunmamaktadır.

- Gerçekçi varsayımlar altında, eklenen yapay gürültü yardımıyla mükemmel gizlilik sağlayabilecektir. Bu da SNR'sinin Bob'unb SNR'sinden daha yüksek olması durumunda bile, Eve'e hiçbir bilgi sızdırılmamasını sağlar.

- Aynı zamanda, mükemmel güvenli bir hizmet sağlamak mükemmel bir gizliliğe her zaman ihtiyaç olmadığı gözlemlenmektedir. Gerçek hayatta, her bir hizmetin diğerlerinden farklı QoS gereklilikleri bulunmaktadır ve Eve'in bu gerekliliklerin altında çalışmasını sağlamamız durumunda, pratik anlamda gizlilik garanti edilebilecektir.

- Uzamsal serbestlik derecesinin (sıfır uzayın) bulunmadığı, kanalın düz sönümleme içerisinde yer aldığı (yani daha fazla ihtimalin olmaması) ve verici tarafta tek bir antenin bulunduğu en zorlu senaryolardan birinde gizliliği sağlayabilecektir.

- Teklif edilen tasarım, sadece gizliliğin arttırılması için değil aynı zamanda PAPR seviyesinin azaltılması ve OFDM tabanlı sistemlerin OOBE seviyesinin hafifletilmesi gibi gizliliğin yanı sıra diğer amaçlar için da faydalanılabilecek eklenen Yapay Gürültüden dolayı kuvvet alanı içerisinde ekstra serbestlik derecesi oluşturmaktadır. Diğer bir deyişle, bu şema, sistem tasarım esnekliğini arttırmaktadır.

- Eve, aynı paketin daha fazla kopyalarını alabilmesi ve bu şekilde şifre çözme kapasitesini arttırabilmesi amacıyla, yeniden iletim istemesi için zorlamak üzere Bob'un sinyallerini karıştırmaktadır (jamming). Ancak şemamızda, Yapay Gürültünün yeniden iletim turlarından her birine eklenmesinden dolayı, Eve'in aynı paketin yeniden iletilen kopyalarından faydalanması önlenecektir. İlgilenen okuyucular, daha fazla bilgi için [7]'ye bakabilirler.

- Teklif edilen şemanın maksimum faydası ve en iyi işletme koşulu, dağıtıcı kanallar üzerinden OFDM tabanlı dalga formlarıyla kullanıldığında elde edilebilecektir. Bunun iki sebebi bulunmaktadır: 1) Yapay Gürültü vektörünün rastlantısallığı sadece kaynakta oluşturulan sinyalin değil aynı zamanda dağıtıcı kanal rastlantısallığının da bir fonksiyonu olmaktadır; 2) Yapay

Gürültü, OFDM'nin ana sakıncalarından bazılarının çözülmesi için yeniden tasarlanabilecektir.

Patent literatüründe, fiziksel katman güvenliğiyle ilgili birçok patent belgesi bulunmaktadır. Aşağıda, bunlardan bazı örnekler verilmektedir.

US9686038 numaralı Amerika Birleşik Devletleri patent belgesi gelişme seviyesi başvurusunda, iletilen verilerle birlikte en az bir sinyal bozma (jamming) iletiminin oluşturulması ve hedef bir alıcıya iletilmesi için bir anten dizisi kullanılarak güvenli haberleşme sağlanmasına yönelik bir yöntem açıklanmaktadır.

US7751353 numaralı başka bir Amerika Birleşik Devletleri patent belgesi gelişme seviyesi başvurusunda, planlanan hedef varış yerinden başka bir ya da daha fazla hedef varış yerine gürültü gönderilmesi yoluyla kablosuz iletimin güvenliğinin sağlanmasına yönelik bir yöntem açıklanmaktadır.

US9014665 numaralı Amerika Birleşik Devletleri patent belgesinde, ilgili hedef alıcılara iletim için bir ya da daha fazla veri akışları ile bir ya da daha fazla sinyal bozma (jamming) akışlarının oluşturulmasını içeren bir haberleşme yöntemi açıklanmaktadır.

US2014153723 numaralı Amerika Birleşik Devletleri patent belgesinde, kullanıcı verilerinin güvenlik özelliklerine uygun olarak dönüştürülmesi ve dönüştürülen verilerin haberleşme kanalı için uygun bir format içerisinde işlenmesiyle işlenen verilerin haberleşme kanalına aktarılması için kullanılabilecek bir sistem, cihaz ve fiziksel katman güvenliği yöntemi açıklanmaktadır.

US8433894 numaralı Amerika Birleşik Devletleri patent belgesinde, fiziksel katman güvenlik işleminin gerçekleştirilmesi için bir yöntem ve aparat açıklanmaktadır.

Buluşun yapısal ve karakteristik özellikleri ve tüm avantajları aşağıda verilen yazılan ayrıntılı açıklama sayesinde daha net olarak anlaşılacaktır ve bu nedenle bu değerlendirmenin de bu ayrıntılı açıklama göz önünde bulundurularak yapılması gerekmektedir.

Buluşun Açıklanmasına Yardımcı Şekiller

Şekil 1: ARQ ve OAN ile ARQ kullanıldığı yöntemlere ait Güvenli Verimlilik-SNR (dB) grafiği

Şekil 2: Eve ve Bob'un MRC kullanıldığı ve kullanılmadığı zamanlardaki Paket Hata Oranı (PER)-SNR (dB) grafiği

Şekil 3: Ortalama Yeniden İletim Sayısı-SNR (dB) grafiği

Şekil 4: Eve ve Bob'un MRC kullanıldığı ve kullanılmadığı zamanlardaki ARQ ve OAN ile geliştirilen yöntemlerle yapılan analize ait Paket Hata Oranı (PER)- SNR (dB) grafiği

Şekil 5: Eve ve Bob'un MRC kullanıldığı ve kullanılmadığı zamanlardaki ARQ ve OAN ile geliştirilen yöntemlerle yapılan analize ait Ortalama Verimlilik- SNR (dB) grafiği

Şekil 6: ARQ ve OAN ile ARQ kullanıldığı yöntemlere ait Ortalama Verimlilik-SNR (dB) grafiği

Şekil 7: Ortalama Ekstra Yeniden İletim Sayısı (L-1)-SNR (dB) grafiği

Şekil 8: CCDF-PAPR grafiği

Şekil 9: Güç Spektrum Yoğunluğu (dBm / Hz) grafiği

Şekil 10: OFDM durumuna eklenen kanal tabanlı Yapay Gürültünün ihtimalinin verici tarafta rastlantısal oluşan örneklerden ve çok yollu frekans seçimli kanalın ihtimalinden geldiğinin gösterimi

Buluşun Açıklanması

Söz konusu buluş, pratik ve çok etkili bir güvenlik yöntemi ve sistemi açıklanmaktadır. Özelikle, karıştırıcı bir sinyal (yani, Yapay Gürültü) meşru kullanıcının kanal kazanımı ve QoS gereklilikleri esas alınarak, her bir yeniden iletim turunda, iletilen veri paketinin x (2), (4) üzerine (kuvvet alanında) eklenir/ üst üste biner (superimposed). Eklenen karıştırıcı Yapay Gürültü sinyalleri, MRC süreci kullanılarak alıcı tarafında bir araya getirildiklerinde, Eve'in performansı önemli seviyede bozulurken, sadece Bob'un tarafında birbirlerini kompanse edecekleri şekilde tasarlanır. Bunu elde edebilmek için, literatürde mevcut Yapay Gürültü tabanlı güvenlik şemalarının aksine, kanal içerisinde sıfır boşluk olmasına bağlı bulunmayacak şekilde tasarlanmış Yapay Gürültü, birinci ve ikinci yeniden iletim turlarında zaman alanı sinyal vektörünün

üzerine (kuvvet alanı) uygun şekilde eklenir ve böylece birinci ve ikinci turlarda yeni alınan sinyal vektörleri aşağıdaki gibi görünür:

$$\mathbf{y}_{i,1} = h_{i,1}(\mathbf{x} + \mathbf{r}_1) + \mathbf{w}_{i,1} \quad (A)$$

$$\mathbf{y}_{i,2} = h_{i,2}(\mathbf{x} + \mathbf{r}_2) + \mathbf{w}_{i,2} \quad (B)$$

Burada ***yi,1*** ve ***yi,2,*** Eve ya da Bob tarafından birinci ve ikinci turlarda alınan paketleri göstermektedir, **r**1 ∈ CN ×1 (3) ve **r**2 ∈ CN ×1 (5) sırasıyla birinci ve ikinci turlarda eklenen Yapay Gürültü vektörleridir. Alıcı taraftaki MRC sürecinin ardından, **y**ˆi şu şekilde olur:

$$\hat{\mathbf{y}}_i = \mathbf{y}_{i,1} h_{*,1} + \mathbf{y}_{i,2} h_{*} \quad (C)$$

$$\hat{\mathbf{y}}_i = \mathbf{x}\,|h_{i,1}|_2 + |h_{i,2}|_2 + \mathbf{r}_1 |h_{i,1}|_2 + \mathbf{r}_2 |h_{i,2}|_2 + \hat{\mathbf{w}}_i \quad (D)$$

Bu eşitlikten (D), verici taraftaki r1 ve r2 değerlerinin eklenmiş Yapay Gürültünün Şekil 2'nin üs kısmında grafik olarak açıklandığı şekilde sadece Bob tarafında tam olarak iptal edilmesini sağlayacak şekilde tasarlanmasının mümkün olduğunu buluruz.Bunu elde etmek için, r1 ve r2, aşağıdaki şekilde, meşru kullanıcı kanal kuvvetinin (|hb,k |2) ve rastlantısal Yapay Gürültü vektörü g fonksiyonu olarak tasarlanmaktadır:

$$\mathbf{r1} = \frac{\mathbf{g}}{|h_{b,1}|^2} \quad (E)$$

$$\mathbf{r2} = \frac{-\mathbf{g}}{|h_{b,2}|^2} \quad (F)$$

$$\mathbf{g} = \sqrt{0.5\phi}\,((2\mathbf{u} - 1) + j(2\mathbf{q} - 1)) \quad (G)$$

Burada g = [g1 g2 · · · gN]T ∈ CN ×1 örnekleri belirli bir dağılıma göre bağımsız bir şekilde bir sembolden diğerine değişebilecek, rastlantısal bir vektör olarak görülebilir. Bundan dolayı, g aynı zamanda, uzunluğu söz konusu mesajınkine eşit entropiye sahip mesaj uzunluğuna eşit ve alıcı tarafla paylaşılmasına gerek bulunmayan bir tek kullanımlı şifre anahtarı olarak algılanabilecektir.Ayrıca, g tasarımının aşağıda gösterilen konularda serbestlik sağlamasından da bahsedilmelidir: 1) eklenen Yapay Gürültünün yapısının (ya da dağılımının) değiştirilmesi, 2) QoS gereklilikleri esas alınarak gerçekleştirilen, eklenen Yapay Gürültü kuvvetinin ayarlanması; 3) tek tip bir aşama dağlımı ile sürekli bir zarfa sahip olacak şekilde tasarlanması suretiyle eklenen Yapay Gürültüden kaynaklanan PAPR probleminin kontrol edilmesi.

Teklif edilen şemada, g değeri (G) eşitliği içerisinde (QAM sinyali gibi) sabit bir zarfa sahip tek tip bir aşama dağılımına sahip olacak şekilde tasarlanmaktadır, söz konusu eşitlikte, ϕ eklenen Yapay Gürültü vektörünün kuvvetidir (varyansıdır) ve QoS gereklilikleri ile daha sonra gösterilecek hedeflenen güvenlik seviyesi esas alınarak optimize edilir. Genelliği kaybetmeden, g değeri, PAPR içerisindeki sıfır artıştan kaynaklandığı üzere, tek tip aşama dağılımında sabit zarf bulunmasından dolayı, PAPR probleminden kaçınılabilecek şekilde tasarlanmaktadır.Bu elde edebilmek için, u ve q vektörleri, bir ve sıfır değerlerine sahip Bernoulli dağılımlı rastlantısal değişkenler olacak şekilde seçilmektedir.Ayrıca, literatürde mevcut Yapay Gürültü tabanlı güvenlik yöntemlerinin birçoğunun, sadece, sabit bir zarfa sahip olmadığından dolayı PAPR seviyesinde önemli bir artışa yol açan, Gaussian dağılımlı gürültü kullandıkları da vurgulanmalıdır.Bilgimiz dahilinde, PAPR problemi mevcut Yapay Gürültü tabanlı güvenlik yöntemlerinde genellikle ihmal edilmişken, bu çalışma bu probleme ışık tutmakta ve bu soruna yönelik pratik bir çözüm sunmaktadır.

Alıcı taraflarda, gerek Bob gerekse Eve tarafında tespit edilen veri sinyali vektörleri, sırasıyla şu şekilde olmaktadır:

$$\mathbf{x}_{\square}^{\square=\mathrm{x}} + \frac{\mathbf{w}_{b}^{\square\square}}{\left|h_{b,1}\right|^{2} + \left|h_{b,2}\right|^{2}} \qquad (H)$$

$$\mathbf{x}_{\square}^{\square=\mathrm{x}} + \frac{\mathbf{w}_{e}^{\square+\mathbf{r}1\left|h_{e,1}\right|^{2}} + \mathbf{r}2\left|h_{e,1}\right|^{2}}{\left|h_{e,1}\right|^{2} + \left|h_{e,2}\right|^{2}} \qquad (I)$$

(D) eşitliğindeki **r**1 ve **r**2 değerleri değiştirildiğinde, planlı olarak eklenen Yapay Gürültünün tamamen iptal edilmektedir. Bundan dolayı, (H) eşitliğinde gösterilen, tespit edilen xˆ paketi, eklenen Yapay Gürültü bulunmaması durumunda aynıdır.Bu da Bob'un paket hata oranı (PER) performansının, bu yöntemin kullanılmasının ardından hiçbir şekilde etkilenmeyeceği anlamına gelmektedir.Eve tarafına baktığımızda, Eve'nin Alice'nin kanalını (TDD sistemlerindeki kanalın tahmin edilmesine yönelik sağlam teknikler kullanılmasından dolayı) ya da eklenen Yapay Gürültü vektörü g değerini (haberleşen taraflarla paylaşılmadığından dolayı) bilmemesinden dolayı, Eve tarafından MRC kullanılıp kullanılmamasına bakılmaksızın, önemli seviyede bir bozulma gerçekleşecektir. MRC'yi kullanması

durumunda ise sıfır çıkarmalı süreçten kaynaklanan ilave karıştırıcı gürültü, PER seviyesini etkileyecektir. Diğer taraftan, MRC kullanmaması durumunda, her bir yeniden iletim turuna eklenen Yapay Gürültü, PER değerini otomatik olarak etkileyecektir. Gizlilik seviyesinin teklif edilen şemayla esas olarak eklenen Yapay Gürültü vektörü g değerinden dolayı artmakta olduğu ifade edilebilecektir, ancak kanalın düz sönümleme içerisinde değil zaman, frekans ya da her ikisi içerisinde dağılımlı olması durumunda, ilave gizlilik kaynağı elde edilebileceği de ifade edilmelidir.

Yapay Gürültü, pratik kablosuz hizmeti kullanımı dikkate alındığında, sadece Bob tarafı kanalının değil aynı zamanda talep edilen hizmetin QoS gerekliliklerinin de esas alınması yoluyla yeniden tasarlanabilecektir.Bundan dolayı sadece, Bob'un performansı Yapay Gürültü eklenmesinden önceki seviyede tutulmaya çalışılırken, Eve'in alım performansını azaltmak için yeterli kuvvete sahip optimum Yapay Gürültü (OAN) eklenmektedir. Aşağıdaki adımlarda, LTE ile gelecekteki 5G ve üzeri ağlar bağlamında teklif edilen güvenlik yönteminin nasıl çalışacağı ve kullanılacağı özetlenmektedir:

QOS BAŞVURU TABLOSU

Hizmet	Gecikme	L	PERt	SNRet	ϕ
Ses	100 ms	2	10- 2	30 dB	0.01
Video	150 ms	3	10- 3	40 dB	0.001

1. Verici (Enode-B), meşru kablosuz kullanıcısının hangi hizmeti kullanmak istediğini tespit eder.
2. Enode-B (Alice), talep edilen hizmete göre, Tablo I'da sunulan başvuru tablosundan, talep edilen hizmetin meşru kullanıcıya güvenilir bir şekilde sağlanması için gerekli olan bir PER eşik değerini (PERt) tespit eder.
3. Enode-B, tespit edilen PER değeri esas alınarak, Eve için elde edilen kapsamlı çevrimdışı PER simülasyon sonuçlarından, Eve'in hizmeti güvenilir bir şekilde gizlice dinlenmesi için gerekli SNR değerini tespit eder (SNRe)

4. Enode-B, bu şekilde bulunan SNR değerinden, bu formülü kullanarak, Eve'in performansının yeterli derecede azaltılması için ihtiyaç duyulan gürültü kuvveti için kabaca optimum bir değer hesaplar $\phi = 10^{\frac{-SNR_A^B(dB)+10}{10}}$.
5. Daha önceden hesaplanan kuvvetle tek tip bir şekilde dağıtılan gürültü, planlı olarak, yukarıda açıklandığı biçimde, sadece planlanan alıcı tarafında bir araya gelmelerinin ardından birbirlerini iptal edecekleri şekilde, birinci ve ikinci yeniden iletim turunda iletilen paketin üzerine eklenir.

Bu yönteme göre, ses ve video gibi günlük olarak kullanılan birçok hizmet içerisinde, tamamen güvenli bir haberleşme sağlamak için aslında mükemmel bir gizlilik seviyesine sahip olmamıza gerek olmadığı görülmektedir. Bunun nedeni, bu yöntemin Eve'in söz konusu hizmetleri kesintiye uğratıp güvenilir bir şekilde kullanmak için gerekli QoS gerekliliklerini elde edemeyeceği bir şekilde çalışmaya zorlamasıdır. Bundan dolayı, sürmekte olan hizmetten faydalanmanın herhangi bir yolu bulunmamaktadır. Başlangıçta güvenilirlik, verimlilik, gecikme ve gizlilik arasında iyi seviyede bir ödünleşme sağlamayı hedeflememize rağmen, yöntemimiz, verimliliğin sadece yarı seviyede azalmasıyla birlikte, tam güvenli mesajlaşma hizmeti sunmak için mükemmel bir gizlilik seviyesi elde edilebileceğini göstermektedir.

Bu da birinci turdaki ilk paket iletiminin her zaman hatalı alınması sağlanırken ikinci turda yeniden iletilen paketin, uygun bir gürültü kuvveti gönderilmesiyle, birinci turda eklenen gürültünün tamamen iptal edilebilmesi suretiyle elde edilmektedir. Bunun, kapsamlı bir simülasyon kullanılmak suretiyle, eklenen Yapay Gürültü varyansının Bob'un SNR değerine eşit seviyede olmasının (yani, ϕ = SNRdB) sağlanmasıyla elde edilebileceği tespit edilmiştir.

Teklif edilen tasarımın, OFDM tabanlı dalga formlarının PAPR ve OOBE değerlerinin azaltılması için kullanılması

Gizlilik seviyesinin yanı sıra, eklenen Yapay Gürültüden aynı zamanda başka faydalar elde etmek üzere de faydalanılabilecektir. Özellikle, eklenen Yapay Gürültü yapış sadece güvenlik sağlamak için değil aynı zamanda OFDM sistemlerindeki

PAPR değerinin azaltılması ve OOBE değerinin hafifletilmesi için de akıllı bir şekilde yeniden tasarlanabilecektir. Burada, yukarıda bahsedilen amaçları elde edebilecek iki yeni tasarımı tartışıyoruz. Birinci tasarımda, Yapay Gürültü sinyali, eklenen Yapay Gürültü kuvvet seviyesiyle tanımlanan belirli bir gizlilik koşuluna tabi olmak üzere, PAPR değerini azaltmak için optimize edilebilecektir; ikinci tasarımda ise, Yapay Gürültü sinyali, dolaylı olarak iyi tanımlanmış bir gizlilik kısıtlamasını temsil edilen bir kuvvet seviyesine tabi olmak üzere OOBE seviyesini en aza indirmek için yeniden tasarlanabilecektir. Ayrıca, teklif edilen güvenlik yönteminin çok taşıyıcılı sistemlerde kullanımıyla, OFDM içerisindeki çok yollu frekans seçmeli kanalların daha fazla ihtimale getirmesinden dolayı, gizli dinlemelere karşı daha dirençli bir yöntem sağladığından bahsedilmelidir. Özellikle, OFDM durumunda eklenen kanal tabanlı Yapay Gürültünün ihtimali sadece verici tarafta rastlantısal olarak oluşturulan örneklerden değil aynı zamanda çok yollu frekans seçimli kanalın ihtimalinden gelmektedir.

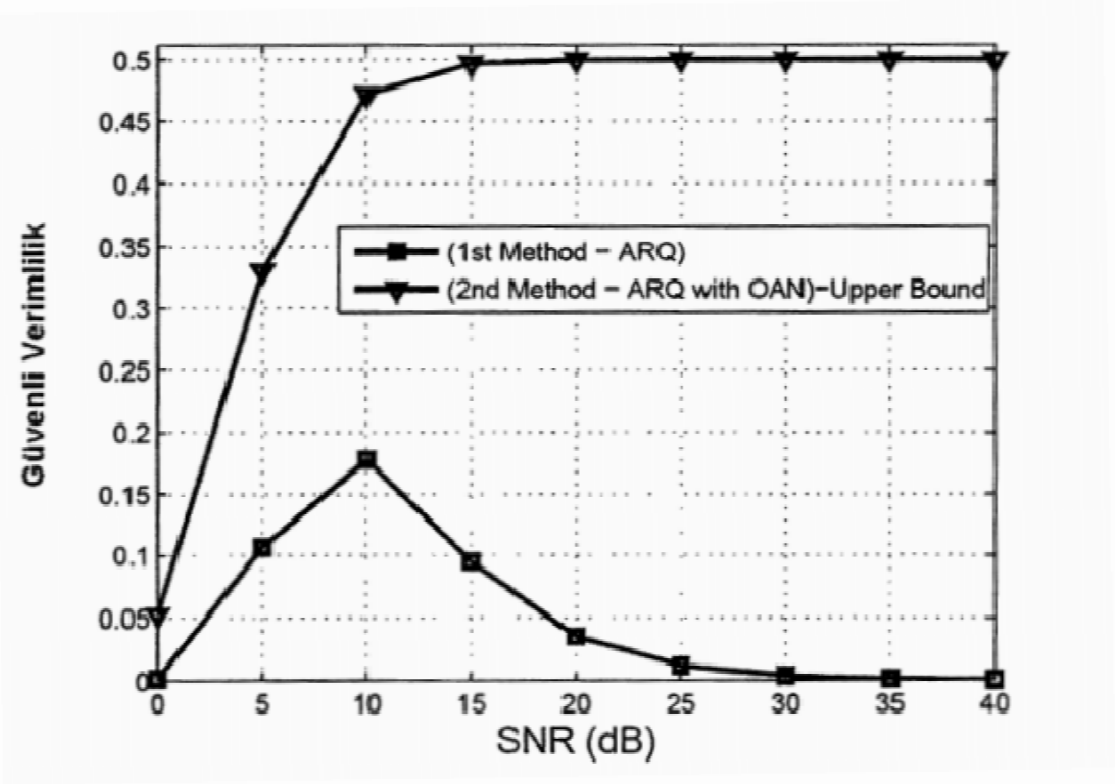
Her istemde bahsi geçen teknik ve diğer tüm özellikleri bir referans numarası takip etmekte olup, bu referans numaraları sadece istemleri anlamayı kolaylaştırmak adına kullanılmıştır, dolayısıyla bunların örneklendirme amaçlı olarak bu referans numaraları ile belirtilen elemanlardan hiçbirinin kapsamını sınırladığı düşünülmemelidir.

Teknikte uzman bir kişinin buluşta ortaya konan yeniliği, benzer yapılanmaları kullanarak da ortaya koyabileceği ve/veya bu yapılanmayı ilgili teknikte kullanılan benzer amaçlı diğer alanlara da uygulayabileceği açıktır. Dolayısıyla böyle yapılanmaların yenilik ve özellikle tekniğin bilinen durumunun aşılması kriterinden yoksun olacağı da aşikârdır.

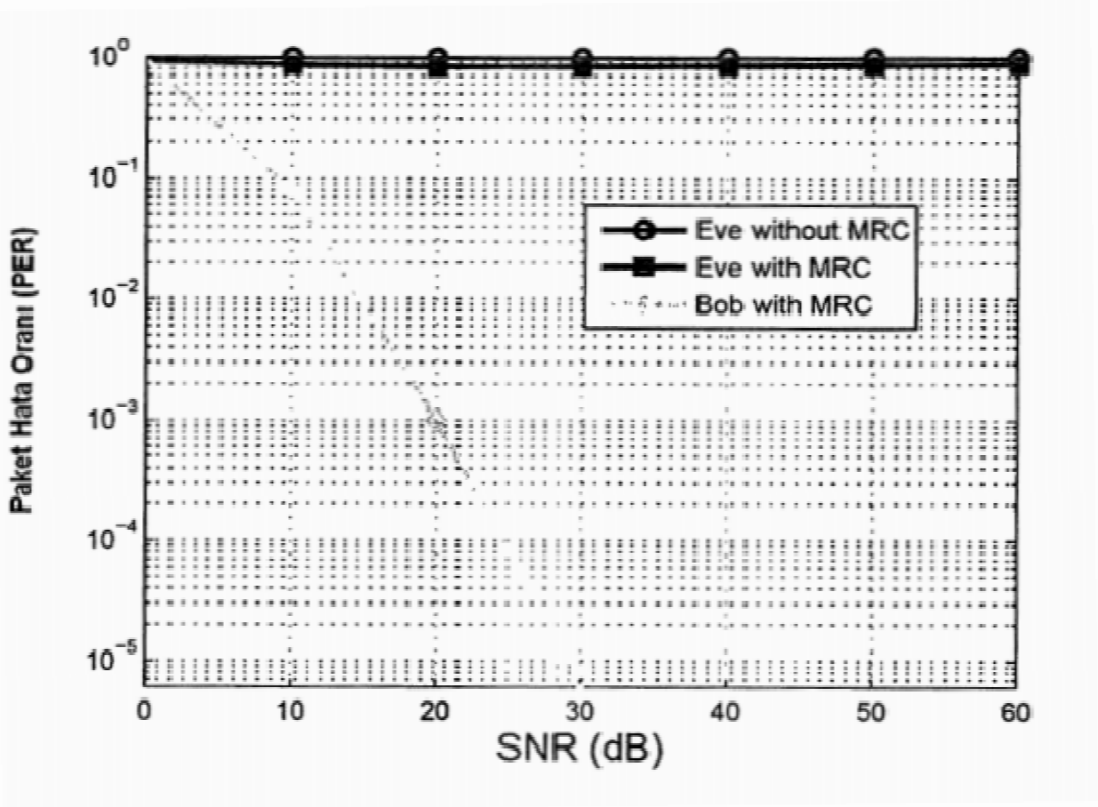
Buluşun Sanayiye Uygulanabilirliği

Açıklanan buluş, büyük bir olasılıkla, gelecek standartlarda uygulanmak üzere, IEEE, 3GPP ve ITU gibi kablosuz standardizasyon topluluklarına teknik avantajları ve faydalarının sunulması yoluyla, endüstriye aktarılabilecektir. Ayrıca, buluş erişim noktaları, baz istasyonları, cep telefonları ve IoT terminalleri dahil olmak üzere

güvenli kablosuz haberleşme cihazlarının yapımıyla ilgili yüksek teknoloji kablosuz güvenlik şirketleri tarafından da kullanılabilecektir. Özellikle, teklif edilen tasarım sağladığı faydalarla birlikte, gelecek güvenli kablosuz sistemler (5G ve üzeri) için iyi bir çözüm adayı olabilecektir.

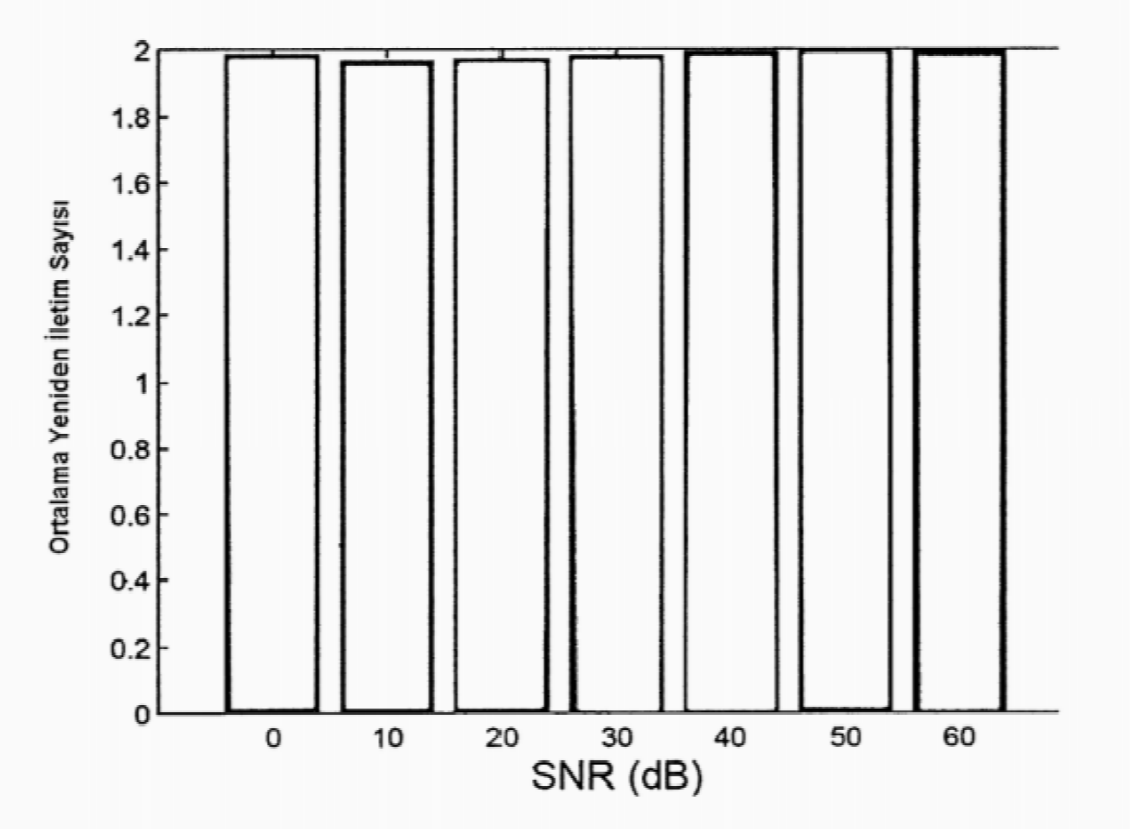


Şekil 1

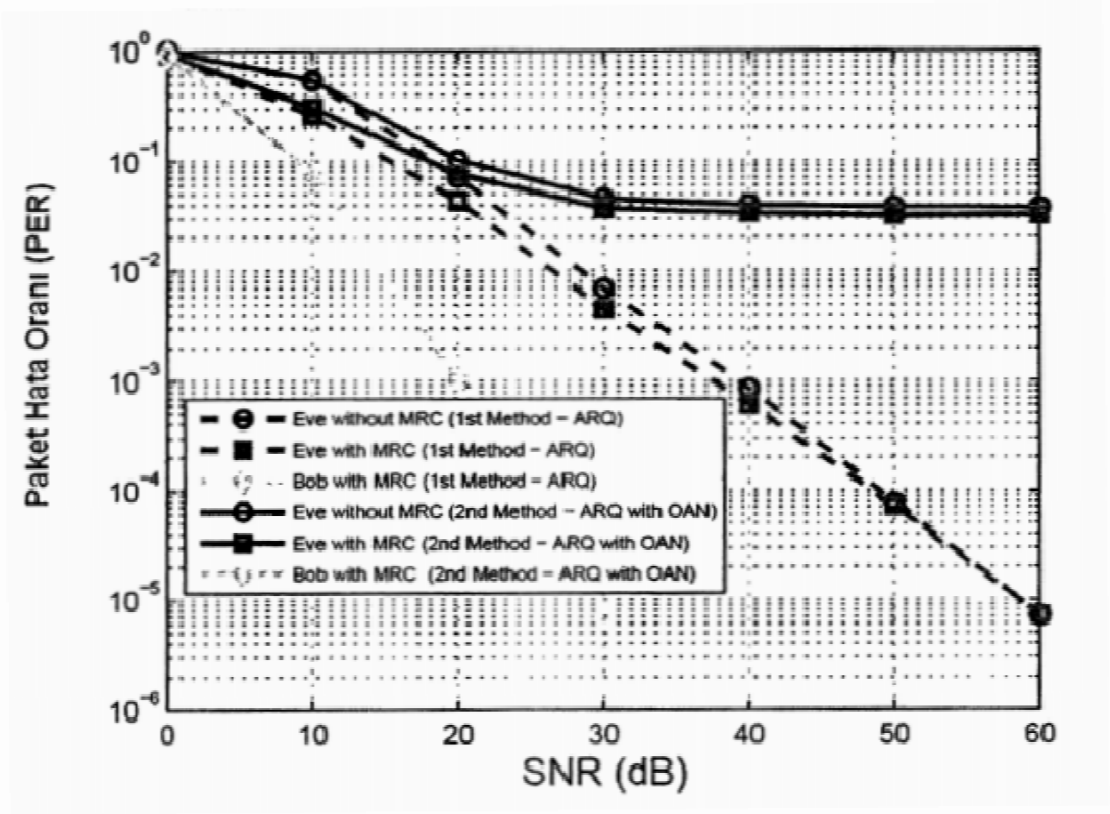


Şekil 2

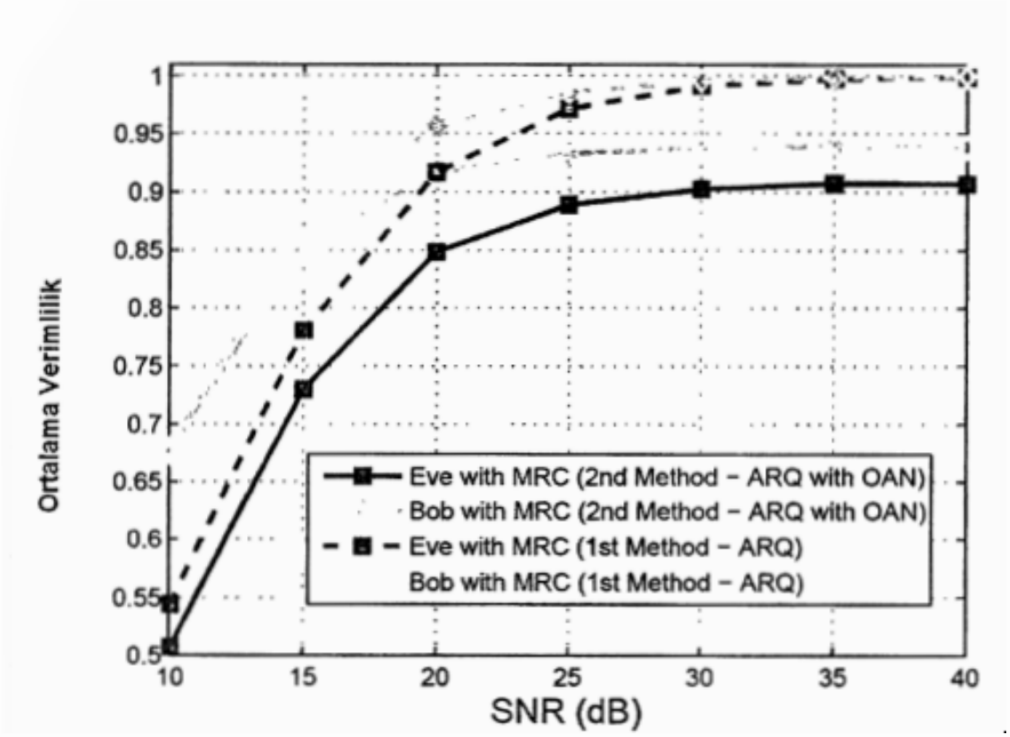
Ş



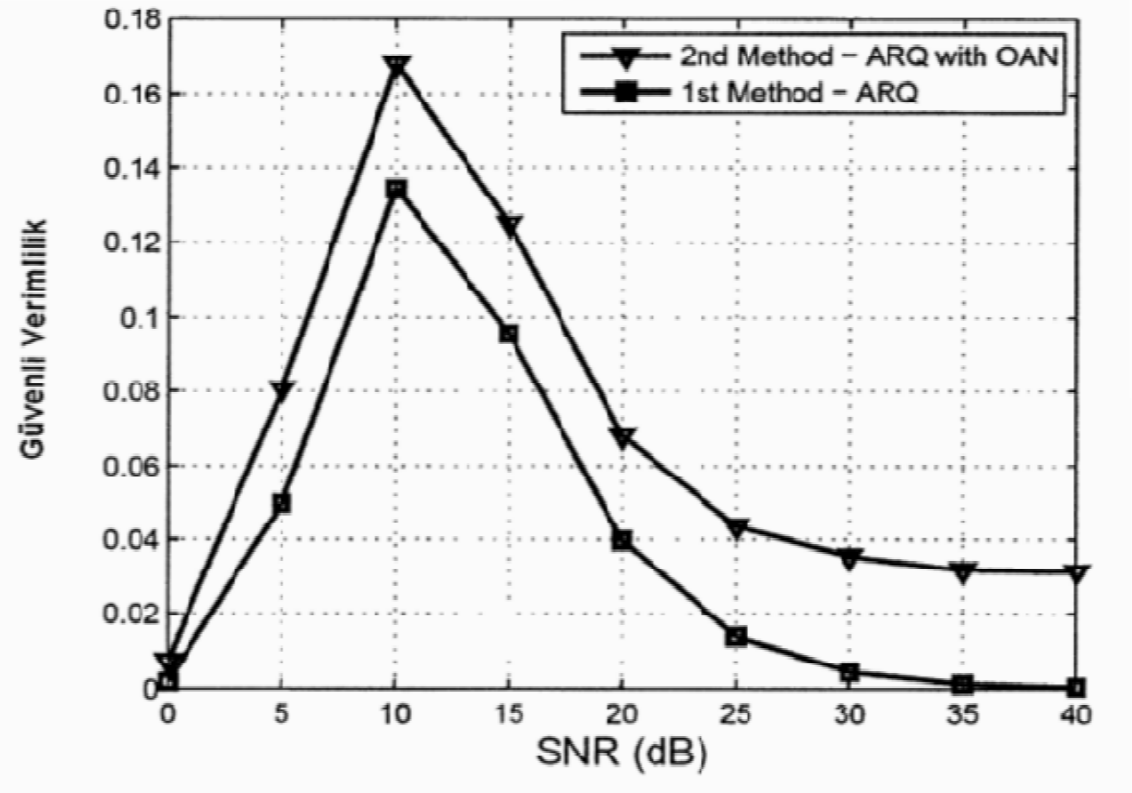
Şekil 3



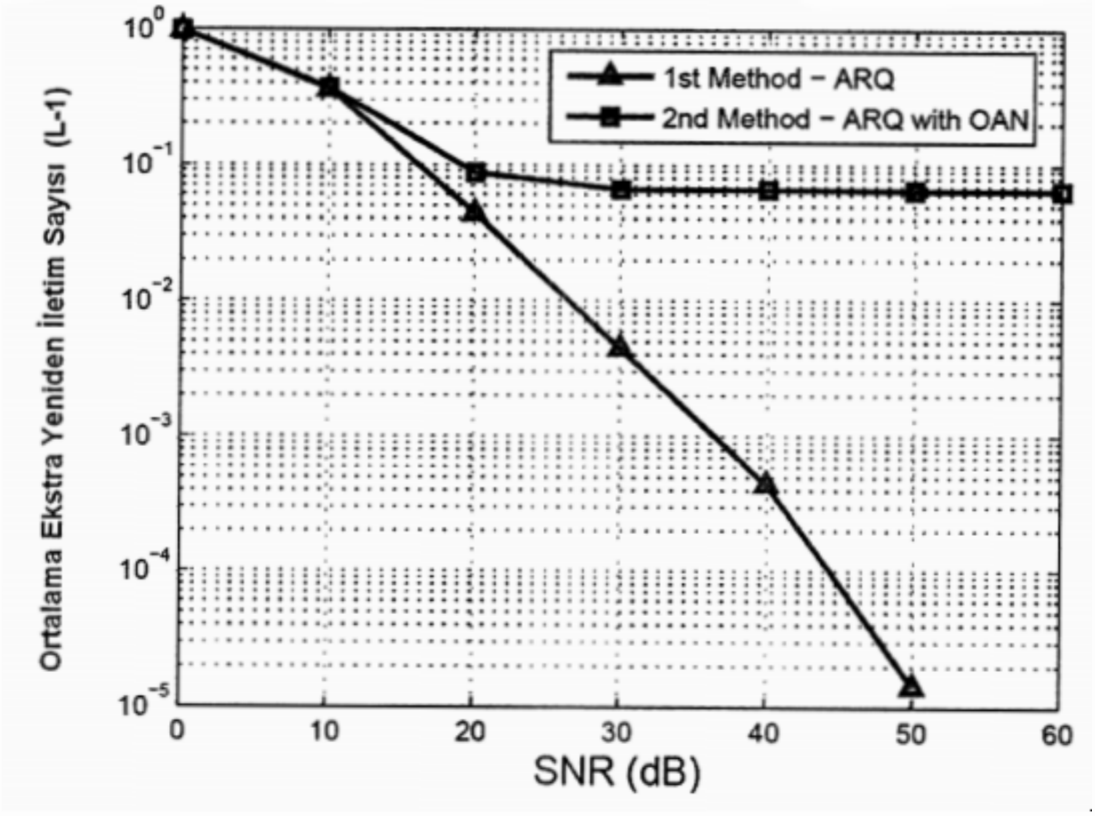
Şekil 4



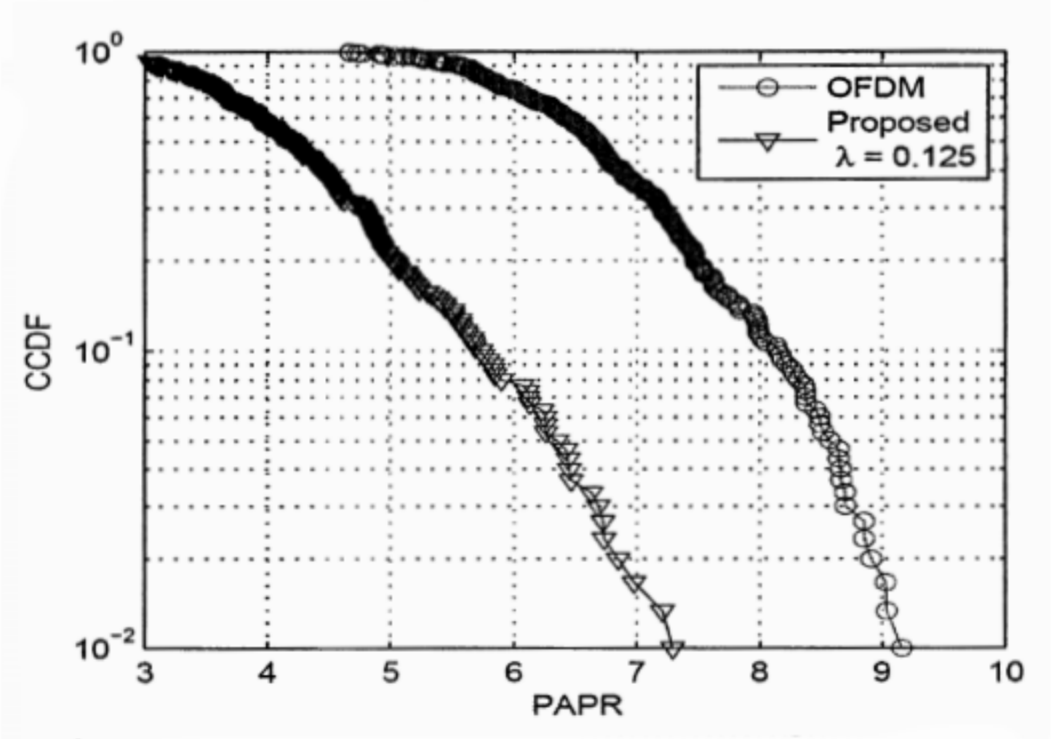
Şekil 5



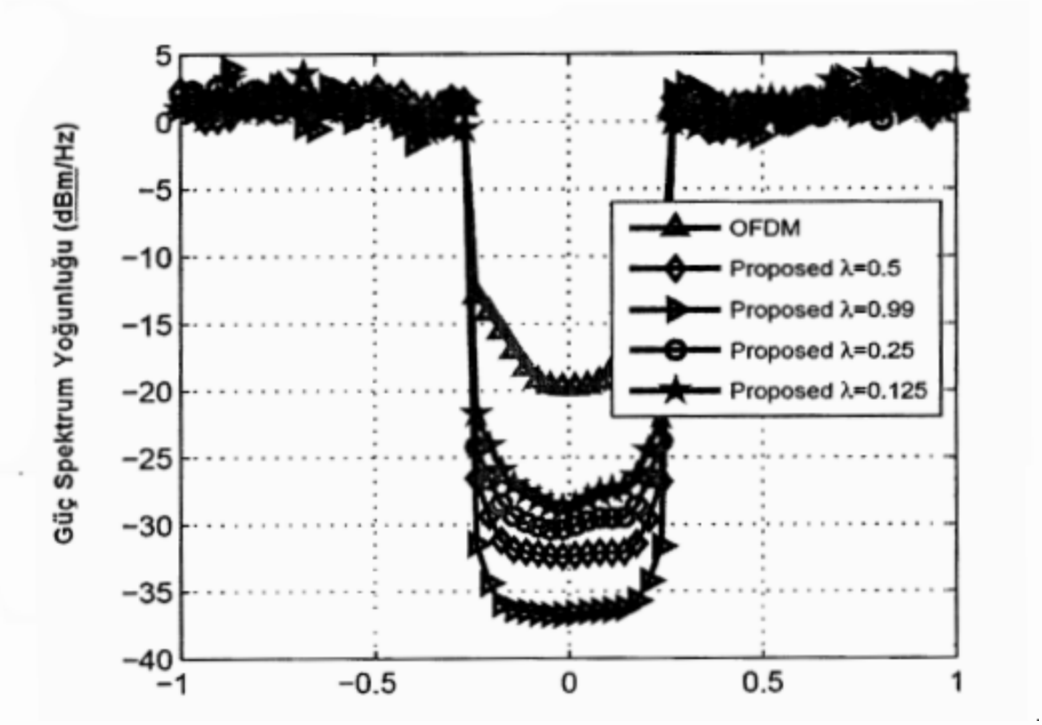
Şekil 6



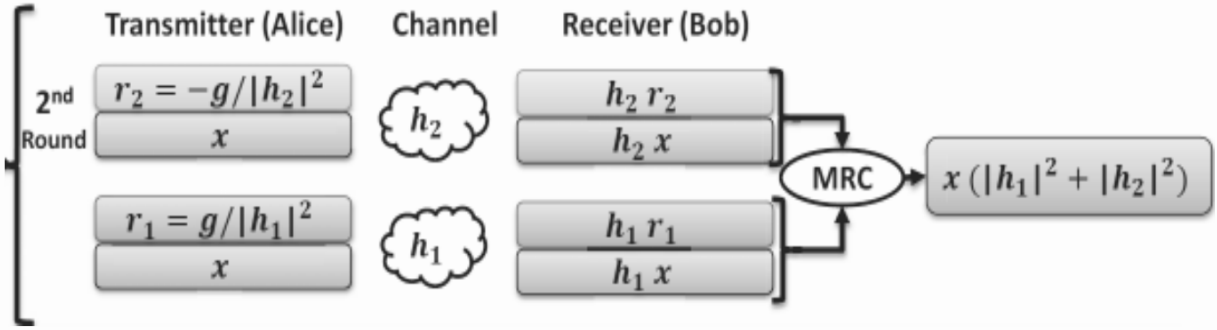
Şekil 7



Şekil 8



Şekil 9



Şekil 10