ÖZET

ORTAK RASTGELE ALT TAŞIYICI SEÇİMİ VE KANAL TABANLI YAPAY SİNYAL TASARIM DESTEKLİ PLS

Mevcut buluş genel olarak Ortak Rastgele Alt Taşıyıcı Seçimi ve Kanal Tabanlı Yapay Sinyal Tasarımı Destekli PLS ile ilgilidir. Kablosuz kanalın rastgeleliğine bağlı olarak fiziksel katman güvenliğini (PLS) sağlamaya yönelik yeni bir yöntem önerilmektedir. Özellikle, kanal tabanlı ortak rastgele alt taşıyıcı seçimi ve yapay sinyal tasarımı, güçlü bir pasif dinleyici varlığında iletişimi korumak için kullanılmaktadır. Analizimiz, her penceredeki en güçlü alt taşıyıcıların seçildiği pencere tabanlı bir alt taşıyıcı seçim yöntemini varsaymaktadır. Seçilen alt taşıyıcılar gizli dizi çıkarma için kabul edilmektedir. Buna ek olarak, oluşturulan kanal bağımlı gizli dizi, hem rastgele alt taşıyıcı seçimi hem de yapay sinyal tasarımı için kullanılmaktadır. Önerilen yöntemin verimliliğini hem mükemmel hem de kusurlu kanal tahmin durumlarında gizli sekans uyuşmazlık oranı (SSDR), çıktı ve bit hata oranı (BER) gibi bazı temsili metrikler aracılığıyla değerlendirmekteyiz. Simülasyon sonuçları sunulmuştur ve kapsamlı görüşmeler gerçekleştirilmiştir.

İSTEMLER

1. Ortak rastgele alt taşıyıcı seçimi ve kanal tabanlı yapay sinyal tasarımı destekli bir fiziksel katman güvenliği (PLS) sistemi olup, özelliği; gizli dizi çıkarma işlemi için her bir pencerenin en güçlü alt taşıyıcılarını kullanan pencere tabanlı bir alt taşıyıcı ve vericinin gizli verilerini korumak amacıyla bilgi verilerine yapay sinyal eklemek için kanal tabanlı rastgele bir alt taşıyıcı seçim şeması olarak iki rastgele alt taşıyıcı seçim şeması içermektedir.

2. İstem 1'e göre bir ortak rastgele alt taşıyıcı seçimi ve kanal tabanlı yapay sinyal tasarımı destekli fiziksel katman güvenliğine (PLS) yönelik bir işletim yöntemi olup, özelliği; aşağıdaki adımlarını içermesidir;

- Tek antenli gerçek bir alıcı kanalında güçlü alt taşıyıcılar bulunması,
- Bulunan güçlü alt taşıyıcılarda nicelleştirme ve gizli sekans oluşturulması,
- Minimum gerekli gizli sekans uzunluğunun (L_{min}) ve L'nin karşılaştırılmasını,
- Karşılaştırma gereken minimum uzunluğu (L_{min}) L'den büyük olması halinde, gizli sekansın yeniden şekillendirilmesi, ardından birinci L_{min} bitlerinin seçilmesi,
- Karşılaştırma gereken minimum uzunluğun (L_{min}) L'den büyük olmaması durumunda ilk L_{min} bitlerinin seçilmesi,
- L_{min} bitlerinin seçilmesinden sonra M uzunluğunda küçük gizli sekans paketlerinin oluşturulması,
- Alt taşıyıcı numarası seçimi için M bitlerinin uzunluğunun N'ye bölünmesi,
- Oluşturulan gizli sekansa göre alt taşıyıcı numarası seçimi yapıldıktan sonra, yapay sinyalin tasarlanması için kanaldan çıkarılan gizli sekansın bilgi verileriyle aynı sırayla modüle edildiği vericinin gizli verilerini korumak için yapay sinyalin bilgi verilerine eklenmesi,
- Semboller arası etkileşimi (ISI) önlemek için zaman alanı şifreli sembollere çevrimsel önek (CP) uyguladıktan sonra iletilen sinyalin gerçek kullanıcıya (tek antenli gerçek alıcı) $\mathbf{X} \in \mathbb{C}^{\mathbf{1}\times \boldsymbol{K}}$ olarak gönderilmesi,
- Sinyalin tek antenli gerçek alıcı tarafında bir $y_b = h_b * x + n_b$ olarak alınması,

- CP'yi çıkardıktan ve zaman alanı tarafından alınan sinyale seri - paralel (S/P) dönüştürmesi uygulandıktan sonra oluşan sinyal üzerinde tek antenli gerçek alıcı ile hızlı Fourier dönüşümü (FFT) kullanılması,
- Sıfırdan kuvvet kanal eşitleme işleminin yapılması,
- Kanal eşitleme prosesi, alınan sinyalin ve kanalının eleman bazında bir $\widehat{X_b} = Y_b \oslash H_b$ olarak bölünmesiyle bulunduktan sonra vericinin sinyalinin (a) tek antenli gerçek alıcılar tarafında alınması,
- P/S dönüşümünden sonra, gerçek alıcının (b), tek antenli gerçek alıcılar tarafından alınan sinyalden yapay sinyali çıkararak, tek antenli gerçek alıcılar ile, bilgi sinyalini oluşturması,
- Bilgi sinyalinin aşağıdaki gibi olacak şekilde çıkarılması,

$$S_b(k) = \begin{cases} \widehat{X_b}(k) - C_b(k), & eğer\ k \in I_{SSC_b}, \\ \widehat{X_b}(k), & diğer\ değerler, \end{cases}$$

- Sinyalin tek antenli dinleyiciler kanalından $y_e = h_e * x + n_e$ olarak yakalanması,
- $\widehat{X_e} = Y_e \oslash H_e$, olarak kanal eşitleme işleminden sonra sinyalin tek antenli dinleyici tarafından alınması,
- Tek antenli gerçek alıcı ile aynı algoritmayı izleyerek kanalına göre tek antenli dinleme yapan kişinin bilgi sinyalinin tek antenli dinleme yapan kişi tarafından oluşturulması,
- Bilgi sinyalinin aşağıdaki şekilde ifade edilen tek antenli bir dinleyicide çıkarılması,

$$S_e(k) = \begin{cases} \widehat{X_e}(k) - C_e(k), & eğer\ k \in I_{SSC_e}, \\ \widehat{X_e}(k), & diğer\ değerler, \end{cases} .$$

3. İstem 2 'ye göre ortak rastgele bir alt taşıyıcı seçimi ve kanal tabanlı yapay sinyal tasarımı destekli fiziksel katman güvenliğine (PLS) yönelik bir yöntem olup, özelliği; burada her

bir pencerede bulunan bütün alt taşıyıcılardan yalnızca güçlü olanları gerçek alıcıda daha güvenilir ve rastgele gizli sekansı çıkarmak üzere seçilmesidir.

TARİFNAME

ORTAK RASTGELE ALT TAŞIYICI SEÇİMİ VE KANAL TABANLI YAPAY SİNYAL TASARIM DESTEKLİ PLS

Teknik Alan

Bu buluşta, kablosuz kanalın rastgeleliğine bağlı olarak fiziksel katman güvenliğini (PLS) sağlamaya yönelik yeni bir yöntem önerilmektedir. Özellikle, kanal tabanlı ortak rastgele alt taşıyıcı seçimi ve yapay sinyal tasarımı, güçlü bir pasif dinleyicinin varlığında iletişimi korumak için tanıtılır. Analizimiz, her penceredeki en güçlü alt taşıyıcıların seçildiği pencere tabanlı bir alt taşıyıcı seçim yöntemini varsayar. Seçilen alt taşıyıcılar gizli sekans çıkarma için kabul edilir. Buna ek olarak, oluşturulan kanal bağımlı gizli sekans, hem rastgele alt taşıyıcı seçimi hem de yapay sinyal tasarımı için kullanılır.

Önceki Teknik

Literatürde sıkışma [1] ve yapay gürültü [2], [10] gibi güvenliği sağlamak için farklı teknikler öneren birçok çalışma bulunmaktadır. Bununla birlikte, bu tür teknikler sadece daha fazla güç tüketmekle kalmaz, aynı zamanda bazı durumlarda iyi tasarlanmamışsa, pik - ortalama güç oranı (PAPR) sorununa neden olmanın yanı sıra gerçek alıcıya da zarar verebilmektedir [3]. Diğer yandan, literatürdeki diğer çalışmalar, yalnızca derinlemesine sönümlü olan ve veri iletimi için yalnızca güçlü alt taşıyıcıların kullanıldığı alt taşıyıcılara gürültü eklemeyi önermektedir, çünkü veri iletimi için tüm bant kullanılmamaktadır [4].

Kablosuz iletimin yayın niteliği nedeniyle, kurallara uygun olmayan kullanıcıların varlığında verilerin güvenliğinin sağlanması kritik bir konu olarak kabul edilmiştir. Fiziksel katman temelli çözümler, esneklikleri nedeniyle başka bir serbestlik derecesi getirmekte, bu da fiziksel katman yöntemlerini bu sorunlarla başa çıkmada umut verici bir çözüm haline getirmektedir. Özellikle, eş zamanlı çift yönlü zaman bölmesi (TDD) modunu kullanarak kablosuz kanaldan [5] gizli sekansı çıkararak güvenliğin sağlanması, bu tür tekniklerde rastgelelik oldukça kritik olduğundan dolayı etkili bir yol olarak tanıtılmıştır [6].

Dahası, zamansal korelasyon, kanal özelliklerinden gizli anahtar çıkarılmasında hayati bir konu olarak kabul edilmiştir [7].

Buluşun Amaçları ve Kısa Açıklaması

Mevcut buluş, yukarıda bahsedilen dezavantajları ortadan kaldırmak ve ilgili teknik alana yeni avantajlar getirmek için ortak rastgele alt taşıyıcı seçimi ve kanal tabanlı yapay sinyal tasarımı destekli fiziksel katman güvenliğine (PLS) yönelik bir yöntem ile ilgilidir. Önerilen yöntem, geleneksel şifreleme tabanlı güvenlik çözümlerine bağlı olmaksızın kablosuz sistemler için güvenli iletişim sağlayabilmektedir. Önerilen algoritma, geleneksel kriptografi yöntemlerinde var olan anahtar paylaşımı gibi fiziksel katman güvenliğindeki kritik sorunu da çözebilmektedir. Ayrıca, bu yöntemde alt taşıyıcı seçimi, başka bir güvenlik katmanı getiren oluşturulan gizli sekansa dayalı olarak rastgele yapılır. Ortak rastgele alt taşıyıcı seçimi ve yapay sinyal tasarımı için önerilen yöntem, kablosuz kanal özelliklerinden gizli anahtar üretimi gibi fiziksel katman güvenlik tekniklerinde hem eş konumlu saldırıları hem de zamansal korelasyon sorununu hafifletmektedir.

Kablosuz kanalın rastgeleliğine bağlı olarak fiziksel katman güvenliğini (PLS) sağlamaya yönelik yeni bir yöntem önerilmektedir. Özellikle, kanal tabanlı ortak rastgele alt taşıyıcı seçimi ve yapay sinyal tasarımı, gerçek kullanıcıdan bile daha güçlü olabilecek pasif bir kulak misafirinin varlığında iletişimi korumak için tanıtılır. Analizimiz, her penceredeki en güçlü alt taşıyıcıların seçildiği pencere tabanlı bir alt taşıyıcı seçim yöntemini varsayar. Seçilen alt taşıyıcılar gizli sekans çıkarma için kabul edilmektedir. Buna ek olarak, oluşturulan kanal bağımlı gizli sekans, hem rastgele alt taşıyıcı seçimi hem de yapay sinyal tasarımı için kullanılır. Önerilen yöntemin verimliliğini hem mükemmel hem de kusurlu kanal tahmin durumlarında gizli sıra anlaşmazlık oranı (SSDR), çıktı ve bit hata oranı (BER) gibi bazı temsili metrikler aracılığıyla değerlendiriyoruz.

Önerilen yöntem, anahtarlarının gerçek düğümlerde paylaşılması gereken geleneksel şifreleme tabanlı güvenlik çözümlerine bağlı olmaksızın güvenli iletişim sağlar. Önerilen yöntem, fiziksel katman güvenliğindeki anahtar paylaşımı gibi geleneksel yöntemlerdeki aşağıdaki sorunları çözebilmektedir:

1. Ağda mevcut olan çok sayıda düğüm nedeniyle gelecekteki kablosuz ağ için anahtar yönetimi ve anahtar paylaşımı zordur.
2. Gelecekteki bazı ağların çeşitli güvenlik gereksinimleri ile farklı hizmet ve senaryoları desteklemesi gerekecektir ve geleneksel şifreleme tabanlı yöntem esnek güvenlik sağlayamamaktadır.
3. Kablosuz kanal özelliklerinden gizli anahtar üretiminde zamansal korelasyon sorununu hafifletme tekniğinde, bu soruna ilişkin kanal zaman içinde çok fazla değişmemektedir.
4. Kurallara uygun düğümde, uygun olmayan düğümde oluşturulan gizli sekansla daha ilişkisiz gizli sekans oluşturmaktadır.
5. Sadece kurallara uygun alıcılar için daha güvenilir gizli sekans oluşturmaktadır.
6. Fiziksel katman güvenlik tekniklerindeki eş konumlu saldırıları hafifletmektedir.
7. Gizli verilere kanal tabanlı yapay sinyal eklenmesi nedeniyle vericinin gizli mesajını gizleyerek güvenli iletişimini sağlamaktadır. Gizli sekans yalnızca kurallara uygun alıcının kanalına dayalı olarak oluşturulduğundan, kurallara uygun olmayan alıcı gizli verilere erişemez. Kurallara uygun olmayan alıcı, kurallara uygun kullanıcıdan yarım dalga boyundan daha uzakta bulunan konumu nedeniyle kurallara uygun alıcı kanalı ile ilişkili olmayan farklı bir kanalla karşılaştığından dolayı kurallara uygun kullanıcı ile aynı gizli sekansı oluşturamaz.

Bu buluşta, önceki çalışmalardan farklı olarak, her penceredeki en güçlü alt taşıyıcıları seçen pencere tabanlı bir alt taşıyıcı seçim yöntemi önerilmektedir. Gizli sekans daha sonra bu seçilen alt taşıyıcılardan oluşturulur. Bu metodolojiyi uygulayarak, kanalın tutarlılık bant genişliği doğal olarak azaltılır, bu da oluşturulan gizli sekansta daha yüksek düzeyde rastgelelik elde etmek için faydalıdır. Ayrıca, kulak misafirinin kafasını karıştırmak için yapay sinyali ve bilgi verilerini taşıyan alt taşıyıcılardan bazılarını seçmek amacıyla rastgele bir alt taşıyıcı seçim yöntemi önerilmektedir. Bu rastgele seçim yöntemi, oluşturulan gizli sekansı, her penceredeki alt taşıyıcı numaralarını temsil etmek için küçük alt bloklara bölerek yapılır. Gizli sekansın rastgeleliği nedeniyle, önerilen alt taşıyıcı seçim şeması tamamen rastgeledir, bu da bir güvenlik açısından fayda sağlar. Son olarak, önerilen yöntemin tüm adımları, sistemin güvenilirliğini ve güvenliğini daha da artıran kurallara uygun kanala dayanmaktadır.

Rastgele iki alt taşıyıcı seçim planı önerilmektedir:

Birincisi, gizli sekans çıkarma için her pencerenin en güçlü alt taşıyıcılarını kullanan pencere tabanlı bir alt taşıyıcı seçimidir. Önerilen yöntem, en güçlü olanlar arasından bazı alt taşıyıcıları seçer. Tüm alt taşıyıcıların kullanılması durumuna kıyasla, bu seçim Eve ile daha ilişkisiz bir gizli sekans sağlar ve aynı zamanda Bob'da daha fazla güvenilirlik sağlar, çünkü her iki düğümde de aynı seçilen alt taşıyıcılara sahip olma şansı azalır. Bu yöntem fiziksel katman güvenlik tekniklerindeki eş konumlu saldırılar sorununu çözmeye yardımcı olur. Diğer yandan, pencere tabanlı şema, tüm alt taşıyıcıların kullanımına kıyasla kurallara uygun kullanıcı kanalında daha ilişkisiz alt taşıyıcılara neden olan bir sekans alt taşıyıcıdan sekans oluşturur. Bu, oluşturulan gizli sekansın rastgeleliğini artırmaya yardımcı olur.

İkincisi, vericinin gizli verilerini korumak için bilgi verilerine yapay sinyal eklemek amacıyla kanal tabanlı rastgele bir alt taşıyıcı seçimidir. Literatürde mevcut olan alt taşıyıcı seçim yöntemlerinin kablosuz kanalın derin sönümleme kısımlarında bulunan alt taşıyıcıları seçmesi dikkat çekicidir. Bununla birlikte, Eve ve Bob'un kanallarının birbirine yakın olduğu bazı durumlar olabilmektedir, bu da bu teknikleri eş konumlu saldırılar nedeniyle güvenli hale getirmemektedir [7]. Bu nedenle, önerilen yöntemimiz Bob'un kanalı tarafından çıkarılan sekansa dayalı olarak alt taşıyıcıları seçerek bu sorunu çözmeyi amaçlamaktadır. Bu durumda, Bob'un ve Eve'in kanalları yakın olsa bile, oluşturulan sekanslar ve seçilen alt taşıyıcılar hala farklıdır.

Gizli verilere yapay sinyal tasarımı eklemek için, yapay sinyale erişimi olmadığı ve alınan sinyalden herhangi bir fayda sağlayamadığı için gizli mesajın dinleyiciden gizlenmesine neden olan bir yöntem önerilmektedir.

Yararlı öngörüler elde etmek maksadıyla temsil edici performans metrikleri araştırılır, örneğin gizli sekans uyuşmazlık oranı (SSDR), bit hata oranı (BER) ve pencere tabanlı alt taşıyıcı seçiminin çıktısı ve tüm alt taşıyıcıları kullanan şema ile karşılaştırması sağlanmıştır.

Aktarma işlemi (.) T, Hadamard bölünmesi ø ile sembolize edilmektedir, kıvrım * ile gösterilmektedir ve |D| D kümesinin kardinalitesi anlamına gelmektedir.

- Önerilen yöntem, yalnızca her penceredeki güçlü alt taşıyıcılardan bit çıkararak daha güvenilir gizli sekans sağlar. (her penceredeki tüm alt taşıyıcılar arasında en yüksek kanal kazancına sahip olan alt taşıyıcılar).
- Önerilen algoritma, bu yöntemlerin tüm gerçek düğümlerde gizli anahtar paylaşımından muzdarip olduğu geleneksel şifreleme tabanlı güvenli çözümlere bağlı olmaksızın güvenli iletişim sağlar.
- Önerilen algoritma, kablosuz sistemler için esnek güvenlik sağlamak için geçerlidir.
- Önerilen yöntem, yapay sinyale erişimi olmadığı ve alınan sinyalden herhangi bir fayda sağlayamadığı için gizli verilere yapay sinyal tasarımı eklemek için, vericinin gizli mesajının dinleyiciden gizlenmesine neden olan bir yol sunmaktadır.

Şekillerin Açıklaması

Şekiller, şekillerin aşağıda tarif edildiği mevcut buluş tarafından geliştirilen ortak rastgele alt taşıyıcı seçimini ve kanal tabanlı yapay sinyal tasarımı destekli fiziksel katman güvenliğini (PLS) daha fazla açıklamak için kullanılmıştır:

Şekil 1: Tek antenli bir verici (Alice), tek antenli kurallara uygun bir alıcı (Bob) ve tek antenli bir dinleyiciden (Eve) oluşan sistem modelidir.

Şekil 1'de:

A: Alice olarak adlandırılan vericidir

B: Bob olarak adlandırılan kurallara uygun alıcıdır

E: Eve olarak adlandırılan dinleyicidir

1: Kanal tahmini amacıyla kullanılan verici ve kurallara uygun alıcı arasındaki referans sinyalidir.

Şekil 2: Rastgele alt taşıyıcı seçimi için önerilen algoritmanın akış şeması.

Şekil 3: Önerilen teknikte bozuk kanal karşılıklılığının çıkarılan gizli sekans üzerindeki etkisi.

Şekil 3'te:

SNR(dB): Sinyalin gürültüye oranıdır.

e: Bozuk kanal karşılıklılık seviyesini göstermek için kullanılan gürültü gücüdür.

Bob: Kurallara uygun kullanıcıdır.

Şekil 4: Önerilen pencere tabanlı alt taşıyıcı seçim yöntemi ile gizli sekans çıkarma için tüm alt taşıyıcıları kullanan şema arasındaki SSDR karşılaştırması: a) e=1, b) e=0.1.

Şekil 4'te hem a hem de b bölümü için:

SSDR: Gizli sekans uyumsuzluk oranıdır.

Q: Gizli sekans oluşturmak için seçilen güçlü alt taşıyıcılara uygulanan nicelleştirme seviyesidir.

SNR(dB): Sinyalin gürültüye oranıdır.

Şekil 5: Önerilen yaklaşımın veri hacmi performansı

Şekil 5'te:

SNR(dB): Sinyalin gürültüye oranıdır.

e: Bozuk kanal karşılıklılık seviyesini göstermek için kullanılan gürültü gücüdür.

Bob: Kurallara uygun kullanıcıdır.

Eve: Dinleyicidir.

Şekil 6: Önerilen yaklaşımın BER performansıdır.

Şekil 6'da:

BER: Bit hata oranıdır.

SNR(dB): Sinyalin gürültüye oranıdır.

e: Bozuk kanal karşılıklılık seviyesini göstermek için kullanılan gürültü gücüdür.

Bob: Kurallara uygun kullanıcıdır.

Eve: Dinleyicidir.

Buluşun Ayrıntılı Açıklaması

Buluşun yeniliği, buluşun kapsamını sınırlamayan ve sadece buluşun konusunu açıklığa kavuşturmayı amaçlayan örneklerle tarif edilmiştir. Mevcut buluş aşağıda ayrıntılı olarak açıklanmıştır.

Fiziksel katman güvenliğine yönelik yeni bir yöntem sunulur. Kanal tabanlı rastgele alt taşıyıcı seçimi ve yapay sinyal tasarımı önerildi. Bu alt taşıyıcı seçim yönteminin daha ilişkisiz alt taşıyıcılarda belirtildiği gibi, oluşturulan gizli sekansta elde edilen pencere tabanlı alt taşıyıcı seçimine bağlı olarak yüksek düzeyde rastgelelik sağlar. Ayrıca, bu yöntem sadece kurallara uygun düğümde oluşturulan gizli sekans için güvenilirliği geliştirmiştir. Son olarak, önerilen pencere tabanlı alt taşıyıcı seçim yöntemi, gizli sekans çıkarma için tüm alt taşıyıcıları kullanan şema ile karşılaştırıldı ve sonuçlar yöntemimizin etkinliğini ortaya koymuştur. Gelecekteki çalışmalar için pasif dinleyici yerine aktif dinleyici düşünülebilmektedir. Önerilen yöntemde, kanal tahmini amacıyla pilot sinyaller gönderirken gerçek kullanıcıyı bulmak zordur.

Sistem modeli:

Tek antenli bir verici (Alice), tek antenli kurallara uygun bir alıcı (Bob) ve tek antenli bir dinleyiciden (Eve) oluşan sistem modelidir.

Bu patentte ele alınan senaryo, gizli bir veri gönderen ve Eve adında pasif dinleme yapan bir kişinin varlığında Bob adlı kurallara uygun bir kullanıcı ile gizli iletişim kuran Alice adlı bir verici içermektedir. Eve'in amacı sinyallerle ilgili kendi gözlemleri aracılığıyla Alice ve Bob arasındaki iletişim bağlantısından gizli mesaj içeriğine erişmektir. Eve, birden fazla antene, daha fazla güce, çevrimdışı işleme, donanım yeteneklerine ve daha iyi sinyal işleme becerilerine sahip olma anlamında Bob'dan daha güçlü olabilmektedir ve konumu verici tarafından bilinmez. Bob ve Eve'in kanallarının birbirinden bağımsız ve ilişkisiz olduğu varsayılmıştır, bu da Eve'in Bob'dan en az yarım dalga boyu uzakta olduğu anlamına gelmektedir. Ayrıca, alınan tüm sinyaller Rayleigh frekans seçici sönüm kanalını deneyimlemektedir. Bob'un kanal durumu bilgisinin (CSI) bir TDD sisteminde karşılıklılık özelliği kullanılarak Alice'de bilindiği varsayılmaktadır, ancak Alice'in Ev'in kanalı hakkında pasif olduğu için herhangi bir bilgisi yoktur. Bu nedenle TDD modunda Alice ve Bob, Alice'ten Bob'a ve Bob'dan Alice'e arasındaki kanalların birbirleriyle ilişkili olduğu varsayılmaktadır [8].

Düşünülen senaryoda, Bob önce Alice'e bir referans sinyali göndermektedir. Daha sonra Alice, bu referans sinyalini kullanarak Bob ile arasındaki kanalı tahmin eder. Uydu - yer bağı kanalının uzak yükleme bağlantısından [9] elde edildiği TDD modunda kanal karşılıklılık özelliğinden yararlanılarak kanalın paylaşılmasına gerek yoktur. Önerilen yöntem, dikey frekans bölmeli çoğullama (OFDM) sisteminin kullanılmasına dayanmaktadır. BPSK modülasyonu kullanılarak eşleştirilen bitler, pasif bir Eve'in varlığında Alice tarafından Bob'a gönderilmektedir. K uzunluğuna sahip frekans alanı, karmaşık veri sembolleri ile temsil edilmektedir . $S = [S_1, S_2, \dots, S_K]$ burada $S \in \mathbb{C}^{1\times K}$ 'dir.

A. Gizli Sekans Çıkarma:

Bob ve Eve tarafından deneyimlenen kanalın frekans yanıtı, sırasıyla $H_b \in \mathbb{C}^{K\times 1}$ ve $H_e \in \mathbb{C}^{K\times 1}$ 'dir, burada K kanal uzunluğunu göstermektedir. Gizli sekans, önerilen pencere tabanlı alt taşıyıcı seçim yöntemi uygulanarak çıkarılır. Bu yöntemde öncelikle pencere uzunluğu (W) belirlenmektedir. Bu uzunluk, her pencerede dikkate alınan toplam alt taşıyıcı sayısını göstermektedir. Buna ek olarak, P, her bir penceredeki tüm alt taşıyıcılar arasında

kazançları en yüksek olan Bob'un kanalının frekans yanıtından seçilen W noktaları arasından (P < W) seçilen alt taşıyıcı sayısı olsun $\mathrm{H_b} = \left[H_{b_1}, H_{b_2}, \ldots, H_{b_K}\right]^{\mathrm{T}}$. Her penceredeki en güçlü alt taşıyıcılara karşılık gelen bu P alt taşıyıcıları, gizli sekansı çıkarmak için Alice tarafından düşünülür. Önerilen pencere tabanlı yöntem, kanaldan yalnızca güçlü alt taşıyıcıları seçer. Seçilen alt taşıyıcıların P sayısının her pencerede sabitlendiği varsayılır. Bu P noktalarından gizli sekansın çıkarılması, Bob'un kanalının rastgeleliğini artırır ve oluşturulan gizli sekansı, dinleyiciyi daha ilişkisiz hale getirmektedir. Böyle bir yöntemin Bob'un kanalı ile dinleyicinin kanalı arasındaki korelasyonu azalttığını ve Bob'da otomatik olarak daha seçici bir kanalı ima ettiğini belirtmek gerekmektedir. Bu, maliyet ve karmaşıklığa sahip herhangi bir filtre veya başka herhangi bir teknik kullanmadan yapılır.

B. Rastgele Alt Taşıyıcıların Seçimi:

Hem yapay sinyal hem de gizli veri taşıdığı düşünülen alt taşıyıcıları seçmek için rastgele alt taşıyıcı seçim yöntemi önerilmektedir. $\mathrm{H_b}$'nin her penceresindeki güçlü alt taşıyıcılar seçildikten sonra, seçilen güçlü alt taşıyıcılardan gizli bir sekans oluşturmak için Bob'un kanalı Alice ve Bob tarafından nicelleştirilmektedir. Bob'un kanal kazanç ölçümleri eşit olarak bölgelere ayrılır ve her bölge hem Alice hem de Bob tarafından multibit nicelleştirme seviyelerine nicelleştirilmektedir. Seçilen alt taşıyıcıların her biri bir bit akışına karşılık gelmektedir. Önerilen yöntemde, minimum bir gizli sekans uzunluğu gereklidir ve L_{min}.ile temsil edilmektedir. Bu minimum uzunluk $L_{min} = |I_{TSC}| \times N$ olarak tanımlanır, burada N bir alt taşıyıcı numarasını tanımlayan bit sayısını göstermektedir ve $|I_{TSC}|$ toplam alt taşıyıcı sayısını göstermektedir. W ve N arasındaki ilişki $W = 2^N$ ile tanımlanır. Gizli sekansın uzunluğu seçilen alt taşıyıcı sayısı ile ilgilidir. Başka bir deyişle, pencere uzunluğu, W ve her pencerede kullanılan alt taşıyıcılar P ile ilgilidir. Bu iki parametre göz önüne alındığında, gizli sekans uzunluğunun L, minimum gerekli uzunluktan, $L < L_{min}$.'den daha az olduğu bazı durumlar vardır. Bu durumda, oluşturulan gizli sekans L_{min} olan istenen uzunluğa ulaşacak şekilde yeniden şekillendirilmektedir. Gizli sekansın uzunluğu, minimum gizli sekansının uzunluğundan çıkarılır, L_{min}, daha sonra baştaki gizli sekans örnekleri minimum gerekli uzunluğa ulaşmak için bir ek olarak eklenmektedir. Diğer yandan, $L > L_{min}$ gizli sekans uzunluğu minimum gerekli uzunluktan daha yüksekse, $L > L_{min}$'den rastgele alt taşıyıcılar seçim algoritması için sadece ilk L_{min} bitleri dikkate alınır. Minimum gerekli uzunluğu sağlamak için, L_{min} gizli sekans M uzunluğuna sahip küçük bloklara bölünür. Her alt bloğun uzunluğu, M her penceredeki toplam bit sayısını temsil eder. Bir alt taşıyıcı numarasını temsil

eden bit sayısı, N $M = W \times N$ ile tanımlanmaktadır. Bu gizli sekans kanala bağımlı ve kanal rastgele olduğundan, seçilen alt taşıyıcılar rastgele seçilmektedir. Toplam alt taşıyıcı sayısı $|I_{TSC}|$, rastgele alt taşıyıcı seçim yöntemini uygulayan seçilen alt taşıyıcı sayısı $|I_{SSC}|$olarak ifade edilmektedir. $|I_{SSC}|$ ve $|I_{TSC}|$ arasındaki oran rastgele olan $0 < (\frac{|I_{SSC}|}{|I_{TSC}|}) \leq 1$, olarak tanımlanmaktadır. Bu oran 1'e yaklaştıkça, sistemin güvenlik seviyesi giderek yükselmektedir. Belirli bir alt taşıyıcı numarasının bir pencerede birden fazla kez tekrarlandığı bazı durumlar vardır. Bu durumda bu alt taşıyıcı numarası bir kez sayılır ve tekrarı dikkate alınmaz. Şekil 2, önerilen algoritmanın akış şemasını temsil etmektedir. Önerilen rastgele alt taşıyıcı seçim yönteminin tüm adımlarını ve detaylarını göstermektedir.

C. Yapay Sinyal Tasarımı ve Bilgi Sinyaline Nasıl Eklenir:

Alt taşıyıcılar rastgele seçildikten sonra, kalan alt taşıyıcılar sadece bilgi sinyali taşırken, yapay sinyalin bu özel alt taşıyıcılardaki bilgi sinyaline eklenmesi gerekmektedir. Yapay sinyalin tasarlanması için, kanaldan çıkarılan gizli sekans, bilgi verileriyle aynı sırayla modüle edilmektedir. Yapay sinyal eklemek için önerilen yöntem, aşağıdaki formülle tanımlanır

$$X(k) = \begin{cases} S(k) + C(k), & eğer\ k \in I_{SSC}, \\ S(k), & diğer\ değerler, \end{cases} \quad (1)$$

burada S bilgi sinyalini temsil eder ve C oluşturulan gizli sekanstır ve Issc seçilen alt taşıyıcıların kümesidir. (1)'de k, Issc setine ait olup olmadığını belirten her sembolün indeksini ifade eder. Issc 'ye ait olan k için, modüle edilmiş gizli sekans aynı sekansa sahip bilgi verilerine eklenmektedir. İletilen sinyal $X \in \mathbb{C}^{1\times K}$, semboller arası etkileşimi (ISI) önlemek için zaman alan şifreli sembollere döngüsel önek (CP) uygulandıktan sonra geçerli kullanıcı Bob'a gönderilmektedir. Bob'un tarafında alınan sinyal

$$y_b = h_b * x + n_b, \quad (2)$$

olarak yazılabilmektedir, burada h_b Bob'un zaman alanındaki kanalı, x iletilen sinyal ve n_b Bob'daki sıfır ortalama karmaşık katkı maddesi olan beyaz Gauss gürültüsüdür (AWGN). CP'yi çıkardıktan ve alınan zaman alanı sinyaline, y_b seri - paralel (S/P) dönüşüm

uyguladıktan sonra, Bob ortaya çıkan sinyal üzerinde hızlı Fourier dönüşümünü (FFT) kullanır. Sıfırdan kuvvet kanal eşitleme işlemi yapılır. Kanal eşitleme işleminden sonra Bob'un tarafında alınan sinyal, alınan sinyalin ve kanalının eleman bazında bölünmesi ile bulunur ve

$$\widehat{X_b} = Y_b \oslash H_b, \tag{3}$$

burada H_b Bob'un frekans alanındaki kanalı ve Y_b S/P dönüşümünden sonra alınan frekans alanı sinyali olarak tanımlanmaktadır. P/S dönüşümünden sonra, Bob alınan sinyalden $\widehat{X_b}$. yapay sinyali çıkararak bilgi sinyalini oluşturur,

$$S_b(k) = \begin{cases} \widehat{X_b}(k) - C_b(k), & eğer\ k \in I_{SSC_b}, \\ \widehat{X_b}(k), & diğer\ değerler, \end{cases} \tag{4}$$

Bilgi sinyali, C_b 'nin Bob'da üretilen modüle edilmiş gizli sekans olduğu ve S_b'nin alınan sembollerden $\widehat{X_b}$ çıkarıldıktan sonra veri sembolleri olduğu şekilde gözlemlenmektedir. Ayrıca I_{SSC_b}, Bob'da ayarlanan seçili alt taşıyıcıları ifade eder. Eve aynı zamanda iletilen sinyale x de erişebilmektedir, ve Bob'dan daha güçlü ve daha fazla kabiliyetli olabileceğinden, kanalından kendi gizli sekansı oluşturmak için Bob ile aynı adımları izler. Eve'in kanalından yakaladığı sinyal, H_e olarak tanımlanır.

$$y_e = h_e * x + n_e \tag{5}$$

Burada, h_e zaman alanında Eve'in kanalını belirtmektedir ve n_e sıfır ortalama karmaşık AWGN gürültüsü anlamına gelmektedir. Kanal eşitleme işleminden sonra Eve'in tarafında alınan sinyal,

$$\widehat{X_e} = Y_e \oslash H_e, \tag{6}$$

olarak tanımlanabilmektedir, burada Y_e'nin frekans alanı S/P dönüşümünden sonra alınan sinyaldir ve H_e Eve'in frekans alanındaki kanalıdır. Eve, kanalına göre Bob'la aynı algoritmayı izleyerek bilgi sinyalini üretmektedir. Eve'de çıkarılan bilgi sinyali,

$$S_e(k) = \begin{cases} \widehat{X_e}(k) - C_e(k), & eğer\ k \in I_{SSC_e}, \\ \widehat{X_e}(k), & diğer\ değerler, \end{cases} \quad (7)$$

olarak tanımlanabilmektedir, burada C_e Eve'de modüle edilmiş gizli sekanstır, S_e alınan sembollerden $\widehat{X_e}$, çıkarılan veri sembolleridir ve I_{SSC_e} Eve'de belirlenen seçilmiş alt taşıyıcılardır. Bob ve Eve'in verici Alice'den aldıkları gizli veriyi elde etmek için aynı adımları izledikleri unutulmamalıdır. Alice, Bob'un kanalından çıkarılan gizli sekansı kullanarak veri aktardığından, Bob bu sinyali Eve'in varlığında güvenli bir şekilde alabilmektedir. Eve birden fazla antene ve Bob'dan daha fazla beceriye sahip olmasına rağmen, kendi gizli sekansını çıkartsa bile bilgi verilerine doğru bir şekilde erişemez ve sıkışmış alt taşıyıcıları ve yapay sinyali bulmak için önerilen yöntemi uygulayamaz.

D. Açıklayıcı Vaka:

Bu bölümde, daha fazla bilgi edinmek için açıklayıcı bir vaka sunulmuştur. Pencere uzunluğunun W = 4 ve P = 1 olduğu varsayılır. Önceki metodolojiye dayanarak, parametreler TABLO I'de verilmiştir.

TABLO I. Önerilen rastgele alt taşıyıcı seçim yönteminin bir örneği.

Parametreler: W=4, P=1, M=8, N=2, I_TSC=20, I_SSC=14.	**Her pencerede çıkarılan sekans**	**İlgili alt taşıyıcı numaraları**	**Kabul edilen alt taşıyıcı yapay eklemek için sayılar sinyal**
Birinci pencere	10111001	{2, 3, 2, 1}	{1, 2, 3} → {2, 3, 4}

İkinci pencere	01110111	{1, 3, 1, 3}	{1, 3} → {6, 8}
Üçüncü pencere	11101100	{3, 2, 3, 0}	{0, 2, 3} → {9, 11, 12}
Dördüncü pencere	10001010	{2, 0, 2, 2}	{0, 2}-{13, 15}
Beşinci pencere	00100111	{0, 2, 1, 3}	{0, 1, 2, 3} → {17, 18, 19, 20}

Bu örnekte, gizli sekans için minimum gerekli uzunluk 40 ve 6 nicelleştirme seviyesi dikkate alınarak oluşturulan gizli sekansın uzunluğu 30'dur. Arzu edilen uzunluğa ulaşmak için sekanstan ilk 10 bit uca bir ek olarak eklenmektedir. Elde edilen bitler 8 uzunluğuna sahip küçük alt bloklara bölünür, burada her 2 bit 1'den 4'e bir alt taşıyıcı numarasını temsil eder. Son olarak, seçilen alt taşıyıcıların aynı sekansına sahip belirli modüle edilmiş gizli sekans sembollerinin aynı bilgi sembolleri sekansına eklendiği kabul edilmektedir. TABLO I'de verilen bilgilerden rastgele seçilen alt taşıyıcılar ile toplam alt taşıyıcı sayısı arasındaki oranın 0.7 olduğu ve bu oranın yüksek olduğu sonucuna varılabilmektedir. Bu, alt taşıyıcıların % 70'inin sıkıştığı anlamına gelmektedir, böylece yapay sinyal ve bilgi verilerini taşırlar ve Eve'in bunları bulması bir şekilde imkânsızdır. Kullanan kanal karşılıklılık özelliği nedeniyle, gerçek düğümler arasındaki kanal aynıdır ve Bob verilerini doğru bir şekilde çözebilmek için hangi alt taşıyıcıların sıkıştığını bilmektedir. Bununla birlikte, Eve aynı adımları izlese bile, seçtiği alt taşıyıcılar farklı kanalı nedeniyle Alice ve Bob ile aynı değildir. Bu, Eve'in verilerini doğru şekilde çözmek için doğru sıkışmış alt taşıyıcıları bulamadığı anlamına gelmektedir.

PERFORMANS ANALİZİ VE SONUÇLARI:

Performansı analiz etmek ve önerilen yöntemin verimliliğini kanıtlamak için simülasyon sonuçları sunulmuştur. Önerdiğimiz yöntemin etkinliği bit hata oranı (BER) performansı, gizli sıra uyuşmazlık oranı (SSDR) ve çıktı yoluyla değerlendirilmektedir. Buna ek olarak, önerilen pencere tabanlı alt taşıyıcı seçim yönteminin gizli sekans çıkarma için tüm alt taşıyıcıları kullanan şema ile karşılaştırılması, farklı varyans değerleri için Alice ve Bob'un oluşturulan sekansları arasındaki farklı bit sayısının yüzdesini temsil eden SSDR açısından gerçekleştirilmektedir. Bu özel çalışmada, BPSK modülasyonu bitleri 64 uzunluğundaki iletilen sembollere eşlemek için kullanılır. Hem Bob hem de Eve için, güç gecikme profili bozulan toplam 5 hat sayısına sahip bir Rayleigh sönümleme kanalı oluşturulur. Gizli sekans üretiminin nicelleştirme seviyesi 64 olarak belirlenmiştir. Toplam alt taşıyıcı sayısı 64 olarak kabul edilmektedir. Pencere uzunluğu 4 ve P = 1'dir. Kusurlu kanal karşılıklılığı ve tahmin hatası da dikkate alınmaktadır. Spesifik olarak, Alice ve Bob için tahmin edilen kanal sırasıyla $\widehat{H}_a = H_a + \Delta H_a$ ve $\widehat{H}_b = H_b + \Delta H_b$ olarak ifade edilmektedir. $H_a = H_b$, sırasıyla Alice ve Bob'un gerçek kanallarıdır. Ayrıca, ΔH_a ve ΔH_b, sırasıyla sıfır ortalama ve varyans $\sigma^2 = e \times 10^{-SNR(dB)/10}$ ile Alice ve Bob'un taraflarındaki bağımsız Gauss gürültü vektörleridir. Gizli sekans oluşturma sistemlerinde dikkate alınan en önemli ölçülerden biri rastgeleliktir. Önerilen kanal bağımlı gizli sekansnin rastgeleliği, MATLAB'de rastgelelik komutu, h = runstest(x) için bir çalıştırma testi kullanılarak kontrol edilmektedir. Test sonuçları, beklendiği gibi rastgele sekans için h = 0'dır.

Şekil 3, kusurlu kanal karşılıklılığını varsayarak SSDR'ye karşı iletim SNR'sini çizer. e azaldığında SSDR'nin de azaldığı gösterilmiştir. Örneğin, SNR = 16dB'de, e = 0.1'den e = 0.0001'e, SSDR sırasıyla 0.3622'den 0.0421'e düşer, bu da % 88'lik bir kazançla sonuçlanmaktadır. Şekil 4, önerilen yöntemin SSDR performansını gizli sekansı çıkarmak için tüm alt taşıyıcıları kullanan şema ile karşılaştırmaktadır. Farklı nicelleştirme seviyeleri ve kanal tahmin hataları olarak kabul edilir. Görüldüğü gibi önerilen yöntem, e = 1 olan en kötü durum senaryosunda büyük bir boşluğa ulaşmaktadır. Örneğin, Q = 1024 durumunda SSDR = 0.48 için, Şekil (4a), önerilen yöntemin önerilen yöntemin verimliliğini kanıtlayan yaklaşık 9dB kazancına ulaştığını göstermektedir. SSDR = 0.457 ve Q = 128 olması durumunda önerilen yöntemin yaklaşık 5dB kazanç sağladığının gösterildiği Şekil (4b) için de aynı yorum

geçerlidir. Ayrıca, daha yüksek nicelleştirme seviyesi, her bir alt taşıyıcıdan daha fazla sayıda bit oluşturulması nedeniyle SSDR'yi arttırmaktadır.

Şekil 5 ve 6, veri hacmini ve BER'i farklı kanal tahmin hataları göz önünde bulundurularak SNR ile karşılaştırmaktadır. Önerilen yöntemin, yüksek spektral verimlilik elde edilmesine neden olan veri iletimi için tüm alt taşıyıcıların kullanımından dolayı dikkate alınan sistem için yüksek verim performansı sağladığını unutmayın. Örneğin, SNR = 10 dB'de Şekil 5'te, en kötü durum e = 1 için, Bob'daki verim değeri 0,8443 iken Eve'deki değer 0,5139'dur, bu da önerilen tekniğin gerçek kullanıcıdaki verimde % 40'lık bir kazanıma ulaştığını göstermektedir. Ayrıca, SNR = 20 dB'de Şekil 6'da ve e = 0.01 varsayıldığında, kurallara uygun kullanıcıda BER değeri 0.0233 ve Eve'de 0.5052'dir, bu da önerilen yöntemin Bob'da % 95 BER kazanç sağladığını kanıtlamaktadır. Çıktı ve BER hesaplaması için kullanılan gizli sekans, yüksek SNR değerlerinde, SNR = 40 dB olarak çıkarılmaktadır.

Bu patentte fiziksel katman güvenliğine yönelik yeni bir yöntem sunulmaktadır. Kanal tabanlı rastgele alt taşıyıcı seçimi ve yapay sinyal tasarımı önerildi. Oluşturulan gizli sekansta, pencere tabanlı alt taşıyıcı seçimi nedeniyle yüksek düzeyde rastgelelik elde edildi. Bu alt taşıyıcı seçim yöntemi, yalnızca gerçek kullanıcıda çıkarılan gizli sekansta güvenilirliği geliştiren daha ilişkisiz alt taşıyıcılarda vurgulanmıştır. Sıkışan alt taşıyıcılar Bob'un kanalına dayalı olarak oluşturulan gizli sekansa bağlı olarak seçildi. Son olarak, seçilen alt taşıyıcıların aynı sekansa sahip belirli modüle edilmiş gizli sekans sembollerinin aynı bilgi sembolleri sekansına eklendiği kabul edildi. Önerilen yöntemdeki tüm adımlar Bob'un kanalına dayalı olarak yapıldığından, sadece Bob'da hem güvenlik hem de güvenilirlik sağlanmıştır. Kusurlu kanal karşılıklılık koşulları da dikkate alınmıştır. Ayrıca, simülasyon sonuçları önerilen yöntemin verimliliğini kanıtlayan Bob'un ve Eve'in BER'leri arasında büyük bir gizlilik boşluğu olduğunu göstermiştir. Son olarak, önerilen pencere tabanlı alt taşıyıcı seçim yöntemi, gizli sekans çıkarma için tüm alt taşıyıcıları kullanan şema ile kararlaştırılmıştır ve sonuçlar yöntemimizin etkinliğini ortaya koydu. Gelecekteki çalışmalar için pasif dinleyici yerine aktif dinleyici düşünülebilir. Önerilen yöntemde, bu husus, kanal tahmini amacıyla pilot sinyaller gönderirken gerçek kullanıcıyı bulmak için zordur.

Bu buluş sanayileşmemeye uygulanabilir ve önerilen yöntem, gelecekteki iletişim ağları ve sistemleri için kablosuz sistemlerde güvenli ve güvenilir iletişim sağlamak için kullanılabilir.

Ortak rastgele alt taşıyıcı seçimi ve kanal tabanlı yapay sinyal tasarımı fiziksel katman güvenliği (PLS) olup, burada sistem, gizli sekans çıkarma için her pencerenin en güçlü alt taşıyıcılarını kullanan pencere tabanlı bir alt taşıyıcı seçimi olarak iki rastgele alt taşıyıcı seçim şeması ve vericinin gizli verilerini korumak için yapay sinyali bilgi verilerine eklemek amacıyla kanal tabanlı rastgele bir alt taşıyıcı (PLS) içermektedir.

Ortak rastgele bir alt taşıyıcı seçimi ve kanal tabanlı yapay sinyal tasarımı destekli fiziksel katman güvenliğine (PLS) yönelik bir işletim yöntemi olup, burada yöntem şunları içermektedir;

- Tek antenli gerçek bir alıcı kanalında güçlü alt taşıyıcılar bulunması,
- Bulunan güçlü alt taşıyıcıları ve gizli sekans üretimi üzerinde nicelleştirmeyi,
- Minimum gerekli gizli sekans uzunluğunun (L_{min}) ve L'nin karşılaştırılması,
- Karşılaştırma gereken minimum uzunluk (L_{min}) L'den büyükse, gizli sekansın yeniden şekillendirilmesini, daha sonra ilk L_{min} bitlerinin seçilmesi,
- Minimum gerekli uzunluğun (L_{min}) karşılaştırılması L'den büyük değilse, daha sonra ilk L_{min} bitlerinin seçilmesi,
- L_{min} bitlerini seçtikten sonra, M uzunluğunda küçük gizli sekans paketlerinin oluşturulması,
- Alt taşıyıcı numarası seçimi için M bitlerinin uzunluğunun N'ye bölünmesi,
- Oluşturulan gizli sekansa göre alt taşıyıcı numarası seçimi yapıldıktan sonra vericinin gizli verilerini korumak için yapay sinyali bilgi verilerine eklenmesi,

Bu aşamada;

- Yapay sinyalin tasarlanması için, kanaldan çıkarılan gizli sekans, bilgi verileriyle aynı sırayla modüle edilmektedir,
- İletilen sinyalin semboller arası etkileşimi (ISI) önlemek için zaman alan şifreli sembollere döngüsel önek (CP) uygulandıktan sonra geçerli kullanıcıya (tek antenli geçerli bir alıcı) $X \in \mathbb{C}^{1\times K}$'olarak gönderilmesi,
- Sinyalin tek antenli gerçek alıcılar tarafından $y_b = h_b * x + n_b$ olarak alınması,
- CP'yi çıkardıktan ve alınan zaman alanı sinyaline seri - paralel (S/P) dönüşüm uyguladıktan sonra tek antenli gerçek alıcı ile elde edilen sinyal üzerinde hızlı Fourier dönüşümünü (FFT) kullanması,
- Sıfırdan kuvvet kanal eşitleme işleminin yapılması,

- $\widehat{X_b} = Y_b \oslash H_b$ olarak alınan sinyalin ve kanalının eleman bazında bölünmesi ile kanal eşitleme işlemi bulunduktan sonra vericinin sinyalinin (a) tek antenli kurallara uygun alıcılar tarafında alınması,
- P/S dönüşümünden sonra, gerçek alıcı (b) tek antenli gerçek alıcılardan yapay sinyalin çıkarılarak tek antenli gerçek alıcılar tarafından bilgi sinyalinin üretilmesi,

Bilgi sinyalinin alınmasını,

$$S_b(k) = \begin{cases} \widehat{X_b}(k) - C_b(k), & eğer\ k \in I_{SSC_b}, \\ \widehat{X_b}(k), & diğer\ değerler, \end{cases}$$

- Tek antenli dinleyici tarafından iletilen sinyale erişilebilmektedir ve dinleyici, tekli anten kanalından gizli sekansı oluşturabilmektedir,
- Sinyalin tek antenli dinleyici kanalından $y_e = h_e * x + n_e$ olarak yakalanmasını,
- $\widehat{X_e} = Y_e \oslash H_e$, kanal eşitleme işleminden sonra sinyalin tek antenli dinleyici tarafından alınmasını,
- Tek antenli gerçek alıcı ile aynı algoritmayı izleyerek kanalına göre tek antenli dinleyicinin bilgi sinyalinin tek antenli dinleyici tarafından oluşturulmasını,
- Bilgi sinyalinin tek antenli dinleyiciden çıkarılması aşağıdaki şekilde ifade edilebilmektedir.

$$S_e(k) = \begin{cases} \widehat{X_e}(k) - C_e(k), & eğer\ k \in I_{SSC_e}, \\ \widehat{X_e}(k), & diğer\ değerler, \end{cases}$$

Buluşun yapılandırmaları şunlardır;

- Ortak rastgele bir alt taşıyıcı seçimi ve kanal tabanlı yapay sinyal tasarımı destekli fiziksel katman güvenliği (PLS) sistemi, kablosuz kanal özelliklerinden gizli anahtar üretimi gibi fiziksel katman güvenlik tekniklerinde eş konumlu saldırıları ve zamansal korelasyon sorununu hafifletmeye yardımcı olur.
- Ortak rastgele bir alt taşıyıcı seçimi ve kanal tabanlı yapay sinyal tasarımı destekli fiziksel katman güvenliğine (PLS) yönelik bir yöntem olup, burada her pencerede

bütünden sadece güçlü alt taşıyıcılar gerçek alıcıda daha güvenilir ve yüksek rastgelelik gizli sekansını çıkarmayı seçmiştir.

REFERANSLAR

[1] Z. Bouida, A. Stavridis, A. Ghrayeb, H. Haas, M. Hasna, and M. Ibnkahla, "Precoding-aided spatial modulation for the wiretap channel with relay selection and cooperative jamming," Wireless Commun. Mob. Comp., 2018.

[2] B. He, Y. She, and V. K. N. Lau, "Artificial noise injection for securing single-antenna systems," IEEE Trans. Veh. Technol., vol. 66, no. 10, pp. 9577–9581, 2017.

[3] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," IEEE Commun. Surveys & Tut., 2018.

[4] E. Gvenkaya and H. Arslan, "Secure communication in frequency selective channels with fade-avoiding subchannel usage," IEEE Int. Conf. Commun. (ICC), pp. 813–818, 2014.

[5] A. Badawy, T. Elfouly, T. Khattab, C.-F. Chiasserini, A. Mohamed, and D. Trinchero, "Robust secret key extraction from channel secondary random process," Wireless Commun. Mob. Comp., vol. 16, no. 11, pp. 1389–1400, 2016.

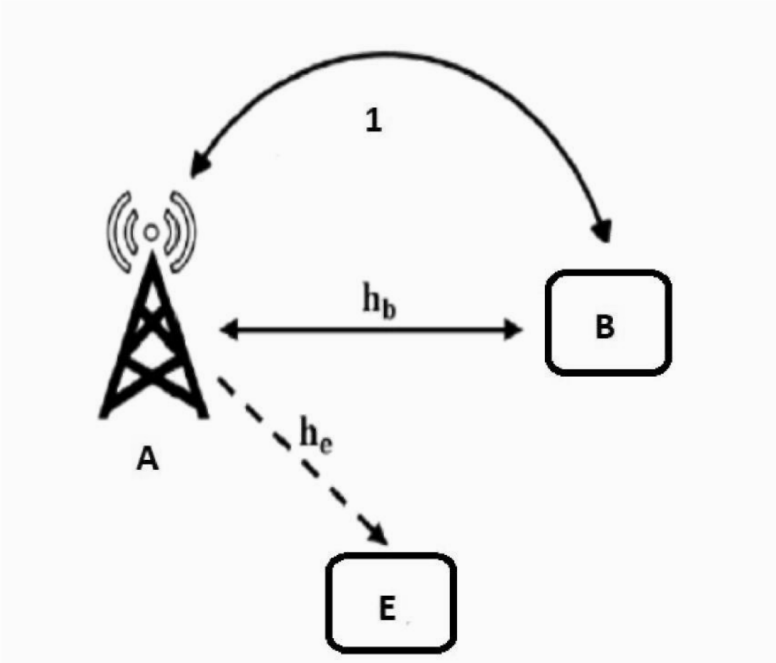
[6] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," IEEE Access, vol. 4, pp. 614–626, 2016.

[7] L. Jiao, N. Wang, P. Wang, A. Alipour-Fanid, J. Tang, and K. Zeng, "Physical layer key generation in 5G wireless networks," IEEE Wireless Commun. Mag., 2019.

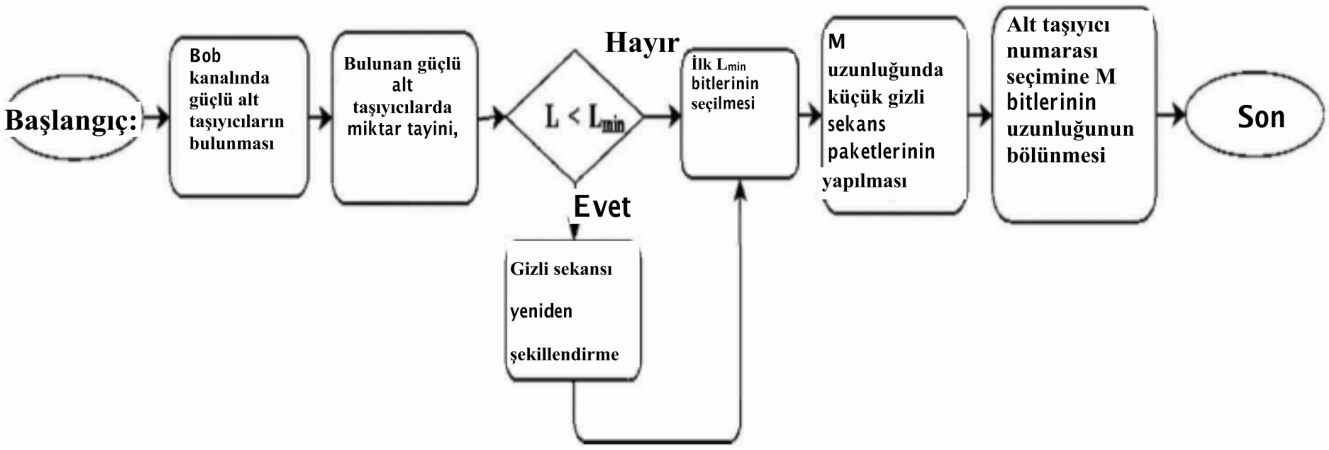
[8] X. Zhou, L. Song, and Y. Zhang, Physical Layer Security in Wireless Communications. CRC Press, 2016.

[9] A. Goldsmith, Wireless Communications. Cambridge University Press, 2005.

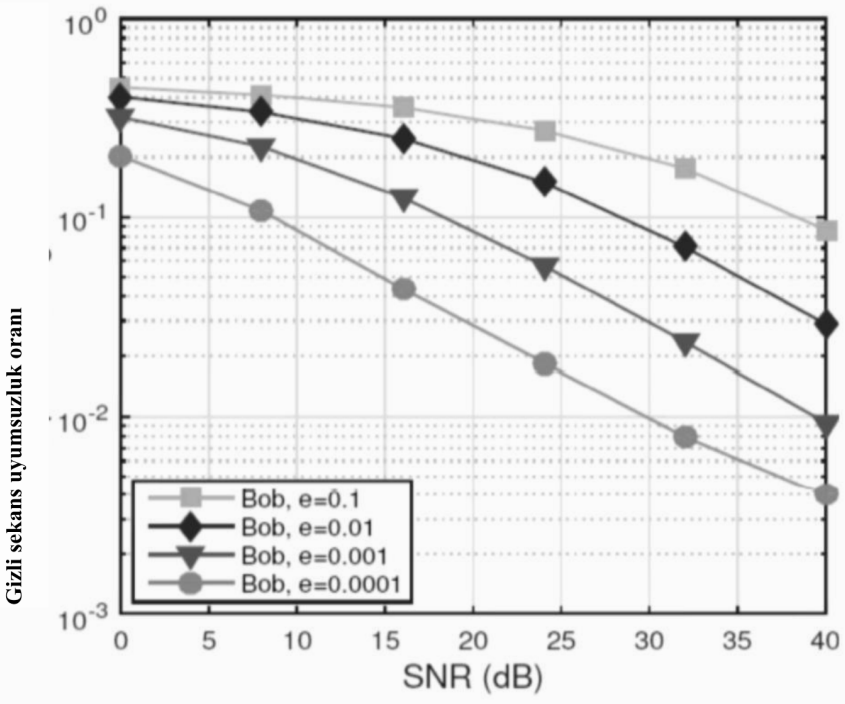
[10] N. Zhao, Y. Cao, F. Yu, Y. Chen, M. Jin, and V. C. Leung, "Articial noise assisted secure interference networks with wireless power transfer," IEEE Trans. Veh. Technol., vol. 67, no. 2, pp. 1087–1098, Feb. 2018.



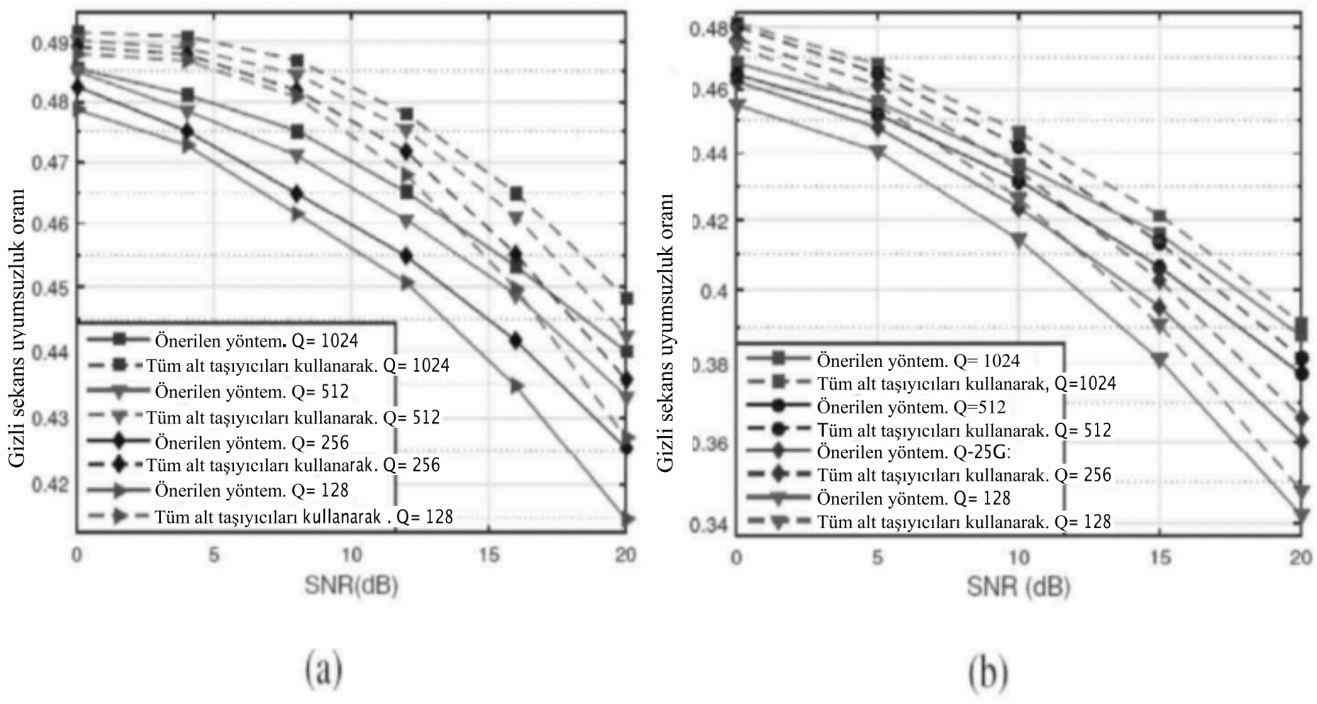
Şekil 1


Başlangıç:
Bob kanalında güçlü alt taşıyıcıların bulunması
Bulunan güçlü alt taşıyıcılarda miktar tayini,
L < Lmin
Hayır
Evet
İlk Lmin bitlerinin seçilmesi
Gizli sekansı yeniden şekillendirme
M uzunluğunda küçük gizli sekans paketlerinin yapılması
Alt taşıyıcı numarası seçimine M bitlerinin uzunluğunun bölünmesi
Son

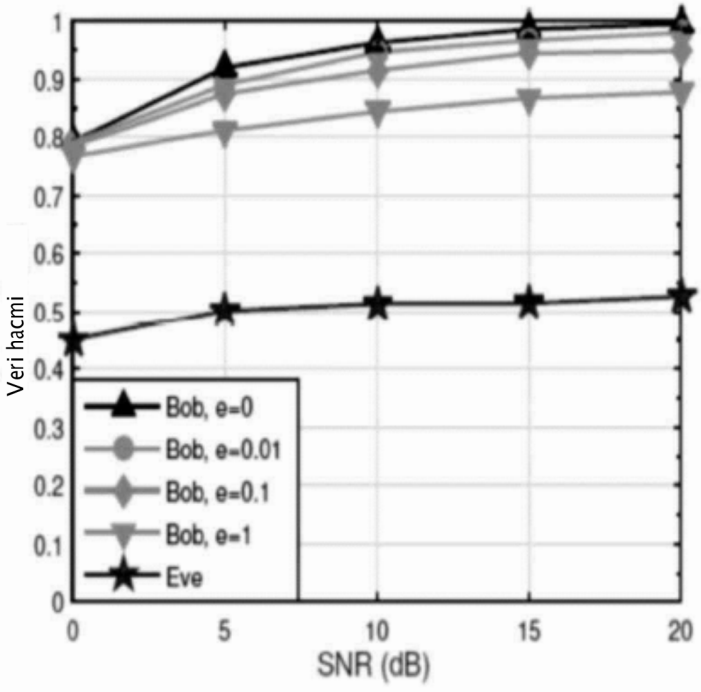
Şekil 2


Gizli sekans uyumsuzluk oranı
10^0
10^{-1}
10^{-2}
10^{-3}
0
5
10
15
20
25
30
35
40
SNR (dB)
Bob, e=0.1
Bob, e=0.01
Bob, e=0.001
Bob, e=0.0001

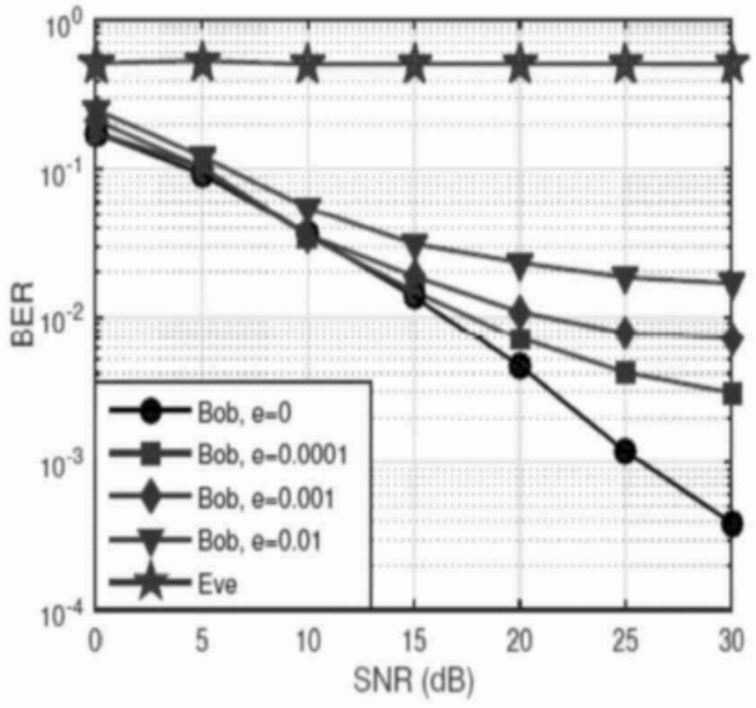
Sekil 3


Gizli sekans uyumsuzluk oranı
SNR(dB)
Önerilen yöntem. Q= 1024
Tüm alt taşıyıcıları kullanarak. Q= 1024
Önerilen yöntem. Q= 512
Tüm alt taşıyıcıları kullanarak. Q= 512
Önerilen yöntem. Q= 256
Tüm alt taşıyıcıları kullanarak. Q= 256
Önerilen yöntem. Q= 128
Tüm alt taşıyıcıları kullanarak . Q= 128
(a)
Gizli sekans uyumsuzluk oranı
SNR (dB)
Önerilen yöntem. Q= 1024
Tüm alt taşıyıcıları kullanarak, Q=1024
Önerilen yöntem. Q=512
Tüm alt taşıyıcıları kullanarak. Q= 512
Önerilen yöntem. Q-25G:
Tüm alt taşıyıcıları kullanarak. Q= 256
Önerilen yöntem. Q= 128
Tüm alt taşıyıcıları kullanarak. Q= 128
(b)

Şekil 4


Veri hacmi
SNR (dB)
Bob, e=0
Bob, e=0.01
Bob, e=0.1
Bob, e=1
Eve
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
0
5
10
15
20

Şekil 5



Şekil 6