Zaman-uzamsal İmzaya Dayalı Güvenli Çok-girişli Çok-çıkışlı Kablosuz Haberleşme Sistemi

SONUÇ RAPORU

Proje No: 114E626

Proje Yürütücüsü:
Yrd.Doç.Dr. Berna ÖZBEK

Araştırmacı:
Doç. Dr. Güneş Karabulut KURT

30 Kasım 2016

İçerik

Şekil Listesi

Tablo Listesi

ÖNSÖZ

Bu rapor TÜBİTAK tarafınadn desteklenen 114E626 numaralı Zaman-uzamsal İmzaya Dayalı Güvenli Çok-girişli Çok-çıkşlı Kablosuz Haberleşme Sistemi başlıklı proje kapsamında yapılan çalışmaları içermektedir.

1 Nisan 2014 ile 30 Eylül 2016 tarihleri arasında İzmir Yüksek Teknoloji Enstitüsü Elektrik-Elektronik Mühendisliği Bölümü ve İstanbul Teknik Üniversitesi Elektronik-Haberleşme Mühendisliği Bölümü'nde gerçekleşmiş olan bu projeye Özgecan Özdoğan, Ozan Alp Topal, Merve Uslu, Mehmet Özgün Demir, Halim Bahadır Tuğrel, Mert Eygi ve Fatih Güleç bursiyer olarak katkıda bulunmuşlardır.

Projemize verdiği desteklerden dolayı TÜBİTAK Elektrik-Elektronik ve Enformatik Araştırma Grubu'na ve emeklerinden dolayı tüm proje çalışanlarına teşekkür ederiz.

Özet

Kablosuz haberleşme sistemlerinde kullanılan kanalın açık bir ortam olması ve iletilen işaretin vericinin kapsama alanı içerisinde kalan her alıcının erişimi dahilinde olması, gizli dinleme türü, pasif güvenlik ihlallerine olanak sağlamaktadır. Bu ihlallere karşı günümüzde kullanılan güvenlik sistemleri, şifreleme çözümlerine dayanmaktadır. Fakat söz konusu verilerin gönderici tarafta şifrelenmesi ve alıcı tarafta şifre çözme işleminin yapılması gecikmeyi daha da arttıracaktır. Bu sebeple şifreleme yöntemleri, gecikmeye duyarlı gerçek zamanlı iletişim sistemlerinde güvenlik seviyesini yüksek tutacak düzeyde yapılamamaktadır. Ayrıca şifrelemede oluşan hesaplama karmaşıklığı, taşınabilir cihazların pil kullanım ömrünü azaltmaktadır. Veri iletimindeki güvenlik seviyesinin arttırılması önemli bir problemdir ve halen çözüm beklemektedir. Yeni nesil haberleşme sistemlerinde kullanılan çoklu antenli yapılar ile uzayda iletim seçiciliği sağlanarak güvenlik çözümleri geliştirilebilir.

Bu projede, çoklu girişli çoklu çıkışlı (MIMO) dikgen frekans bölmeli çoğullama (OFDM) tabanlı kablosuz haberleşme sistemlerinde uzay, zaman ve frekanstaki seçicilik özelliklerini kullanarak kanal imzaları hem iç mekan ve hem de dış mekan uygulamaları için çıkartılmıştır. Yetkili kulllanıcıya iletilecek verinin güvenliğinin sağlanması ve gizli alıcılar tarafından sezinlenme olasılığı azaltmak için kablosuz kanalın faz ve genlik bilgisi nicemlenmiş ve hüzmeleme yöntemi gerçekleştirilmiştir.

Projemiz iki iş paketi olarak planlanmış ve her bir iş paketinin hedeflerine ulaşılmıştır. İlk iş paketinde MIMO-OFDM tabanlı kablosuz haberleşme sistemleri için verimli fiziksel katman güvenlik yöntemleri tasarlanmıştır. Geliştirilen kod kitapçığı, kullanıcı seçimi ve önkodlama yöntemleri ile MIMO-OFDM tekniğinin uzay, zaman ve frekans seçicilik avantajı kullanılarak, gizli dinleyici saldırıları mevcut tekniklere göre daha verimli olarak engellenmiş ve güvenlik kapasitesi arttırılmıştır. İkinci iş paketinde ise MIMO-OFDM sistemi için fiziksel katman güvenliğinin yazılım tabanlı radyo düğümleri ile gerçeklenmesi yapılmıştır. Karşılıklı kanal özelliği ile şifreleme için kullanılacak anahtarların uzunluğu belirlenmiş ve güvenlik anahtarı çıkarımı için anahtar hata oranının teorik analizi elde edilmiştir.

Anahtar Kelimeler: Telsiz haberleşme sistemleri, Fiziksel katman güvenliği, MIMO-OFDM, Nicemlenmiş kanal, Yazılım tabanlı radyo birimleri.

Abstract

The broadcast transmission channel of the wireless communication systems and the ability of all users within a coverage range to receive transmitted signals enable passive security breaches such as eavesdropping. Current state of the art security measures rely on encryption techniques. However, the encryption of these data packages on the transmitter side and decryption on the receiver side will further increase the transmission delay. Based on these facts, a required security levels may not always be obtained in delay sensitive real-time communication systems. Additionally the associated computational complexity will also reduce the battery lives of the portable devices. Enhancement of the security levels in data communications is an important problem that is yet to be solved. New security measures can be developed based on the spatial selectivity of the multi-antenna structures used in the next generation communication systems.

In this project, the signatures based on spatial, temporal, frequency properties of the channel has been developed for the multi input multi output (MIMO) orthogonal frequency division multiplexing (OFDM) wireless systems by considering both indoor applications and the outdoor environments. In order to provide the secrecy of the data and the reduce the detection probability of the eavesdroppers, the channel phase and amplitude information has been quantized and beamforming techniques have been implemented with the usage of specific codebook designs.

Two work packages have been successfully completed according to their own objectives. In the first work package, the efficient physical layer security system has been developed for MIMO-OFDM based wireless communication systems. The secrecy capacity has been improved with designed codebook, user selection and beamforming techniques by the space, time and frequency selectivity of the wireless channels, avoiding the eavesdropping techniques in a more effective manner when compared to the existing techniques. In the second work package, the physical layer security system based on MIMO-OFDM has been implemented in a proof-of-concept levels by making use of software defined radio nodes in a wireless network. By this way, the results obtained through simulations have been compared with a real-life system by adjusting the secret key length based on the physical layer security requirements in the designed practically realizable secure MIMO-OFDM system. Besides, we have derived a theoretical expressions for key error rate and we have compared these results with the one obtained through channel measurements via software defined radio.

Keywords: Wireless communication systems, Physical layer security, MIMO-OFDM, Quantized channel, Software defined radio nodes.

1 Giriş

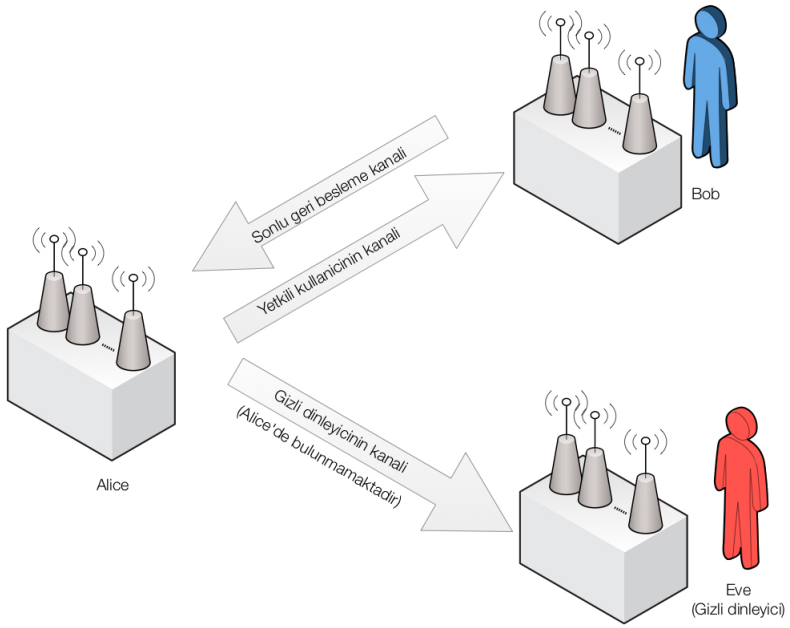
Kablolu iletişim teknolojilerine kıyasla birçok üstünlüğü bulunan kablosuz iletişim son yıllarda büyük gelişmelere sahne olmuştur. Kablosuz iletişim teknolojisini diğerlerinden ayıran nokta ise; iletim ortamı olarak havayı kullanmasıdır. Kablosuz ağların, gönderim ortamı olarak havayı kullanmasından dolayı, kendine özgü kısıtların yanında, güvenlik sorunu da bulunmaktadır. Havada serbestçe yayılan radyo dalgalarının kapsama alanı dahilinde herkesin erişime sahip olması, gizli dinlemeler güvenlik ihlallerine olanak vermektedir. Aynı zamanda, fiziksel katmanda iletişim tekniklerindeki sınırlı seçenekler, ek güvenlik önlemlerini getirmektedir. Kablosuz cihazların ve onlara bağımlılığımızın giderek artmasıyla, güvenlik çözümleri hayati önem taşımaktadır. Bu çözümler, iletişim sistemlerinde sıklıkla kullanılan ve 7 katmandan oluşan OSI referans modelini temel almaktadır. Bir bilginin ele geçirilmesi için tüm katmanlardaki güvenlik önlemleri aşılmalıdır.

Bu çerçevede kablosuz güvenlik çalışmaları son zamanlarda önem kazanarak artmıştır. İlk olarak, bir iletişim düğüm çifti arasında, iletilen bitler, paylaşılmış bir gizli anahtar kullanılarak kriptografik yöntemlere dayalı uygulama katmanında güvenlik protokolleri üzerine kapsamlı çalışmalar vardır. İkinci olarak, güvenli iletişimin orijinal bilgi-kuramsal formülü, Shannon ile kablosuz kanal üzerinde güvenli iletişimin temel limitlerini karakterize ederek inşa edilebilir. Üçüncü olarak ise, kablosuz kanalın ve sistemin niteliklerini kullanarak geliştirilen fiziksel katman güvenlik önlemleri ilgi odağı olmuştur.

Fiziksel katmanda güvenlik methodlarındaki ve çoklu anten sistemlerindeki gelişmeler gelecek nesil haberleşme ağlarında güvenlik sağlanmasının önünü açmıştır. Hüzmeleme ve yapay gürültü (artificial noise-AN) teknikleri Çok Girişli Çok Çıkışlı (Multiple Input Multiple Output-MIMO) dikgen frekans bölmeli çoğullama (OFDM) tabanlı sistemlerde güvenlik kapasitesini arttırmak için kullanılmaktadır. Bu bağlamda alıcılara ait kanal durum bilgisinin vericiye iletilmesi sistemin güvenlik performansı açısından kritiktir.

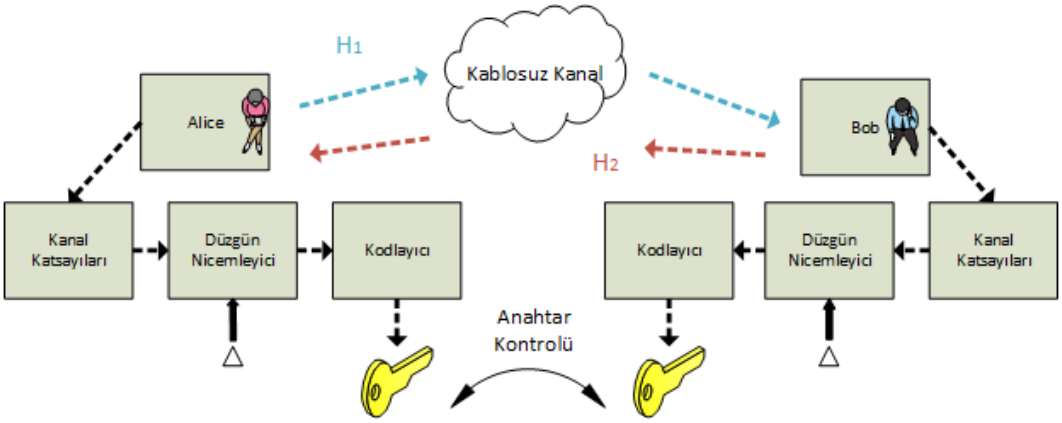
Fiziksel katmanda kanalın karşılıklı olma özelliğinin yardımıyla gizli anahtar üretimi, kablosuz kanalın rastgeleliğine dayanmaktadır ve güvenliğin sağlanması açısından can alıcı noktasıdır. İlaveten, bu özellik sayesinde, basit donanımlar ile, yüksek verimli, düşük hesaplama karmaşıklığına sahip sistemler gerçeklenebilir. Kanalın karşılıklı olma ilkesi, yukarı ve aşağı yönlü bağlantı kanallarının dürtü yanıtlarının aynı olduğunu garantiler. Karşılıklı kanal özelliği ile, gizli anahtar üretimi sağlanarak, anahtar, fiziksel kanal ile yalnızca yetkili alıcıya paylaşılarak, kötü niyetli kullanıcılar için ulaşılamaz hale gelir. Anahtarlar, değişen çevre hareketleri ile dinamik olarak oluşturulur, bu da paylaşılan anahtarın gizliliğini arttırır.

Fiziksel katman güvenliğinde özgün algoritmalar gerçekleştiren projemiz iki iş paketinden oluşmuştur. İlk iş paketinde MIMO-OFDM tabanlı kablosuz haberleşme sistemleri için verimli fiziksel katman güvenlik yöntemleri Şekil 1'deki model gözönüne alınarak geliştirilmiştir. Bu kapsamda, MIMO-OFDM tekniğinin uzay, zaman ve frekans seçicilik avantajlarından yararlanılarak kod kitapçığı, hüzmeleme yöntemi, kullanıcı seçimi ile gizli dinleyicinin yetkili kullanıcıya iletilen veriyi algılaması engellenerek sistemin güvenlik kapasitesi arttırılmıştır. Önerilen algoritmaların tasarımında hem durağan hem de durağan olmayan kablosuz kanal yapıları gözönüne bulundurulmuştur.



Şekil 1: Güvenli MIMO-OFDM sistem modeli

İkinci iş paketinde tasarlanan sistemin konsept ispatı yazılım tabanlı radyo düğümler kullanılarak ve Şekil 2'deki model gözönüne alınarak gerçekleştirilmiştir. Bu kapsamda hüzmeleme methodu MIMO-OFDM sistemi için yazılım tabanlı radyolar üzerinde gerçekleştirilmiş, tek giriş tek çıkış (SISO)-OFDM ve MIMO-OFDM sistemler için karşılıklı kanal özelliği incelenmiş ve anahtar hata oranı teorik analizi gerçekleştirilmiştir.



Şekil 2: Anahtar çıkarım modeli

Bölüm 2'de ayrıntılı bir literatür taraması verilmiştir. Bölüm 3'te proje kapsamında kullanılan gereç ve yöntemler anlatılmıştır. Bölüm 4'te proje amaçları doğrultusundaki bulgular sunulmuştur. Bölüm 5'te ise elde edilen sonuçlar özetlenmiştir.

1.1 Başarı Ölçütleri

Bu projede güvenli MIMO-OFDM sistemleri ele alınmış olup tasarlanan algoritmalar için başarı ölçütleri aşağıda listelenmiştir.

- İş Paketi 1:
  - Birden fazla antenli verici, tek antenli seçilen tek yetkili kullanıcı ve birden fazla antenli gizli dinleyici içeren çoklu giriş tekli giriş (MISO) sistemleri için güvenlik kapasitesinden ödün vermeden geri besleme yükünün azaltılması
  - Durağan olmayan kanallar için birden fazla antenli verici, tek antenli tek yetkili kullanıcı ve birden fazla antenli gizli dinleyicisine sahip MISO sistemler için güvenlik kapasitesinin zamanla azalmasının önlenmesi
  - Birden fazla antenli verici, tek antenli tek yetkili kullanıcı ve tek antenli tek gizli dinleyicisine sahip MISO-OFDM sistemleri için uzamsal ve frekansa dayalı imzasının oluşturulması
  - Birden fazla antenli verici, tek antenli seçilen birden fazla yetkili kullanıcı ve tek ve birden fazla antenli gizli dinleyiciye sahip MIMO sistemleri için hem güvenlik kapasitesi arttırılması hem de aynı zamanda geri besleme yükünün azaltılması.
- İş Paketi 2:
  - Hüzmelemenin MIMO-OFDM sistemleri için yazılım tabanlı radyolarda gerçekleştirilmesi
  - Yazılım tabanlı radyolarda ölçüm sonuçlarına göre hem SISO-OFDM hem de MIMO-OFDM sistemleri için karşılıklı kanal özelliği ile güvenlik anahtarı çıkarımı yapılması
  - Fiziksel katman güvenlik anahtarı çıkarımı anahtar hata oranının teorik analizinin elde edilmesi

1.2 Proje Çıktıları

Proje kapsamında ölçülebilir diğer başarı ölçütleri 1 ulusal konferans, 1 uluslararası konferans ve 1 dergi makalesi yayını, 2 yüksek lisans ve 2 lisans öğrencisinin tezlerine katkıda bulunması, 1 patent başvurusunun yapılması ve proje çıktılarının şirketlere sunulması hedeflenmişti. Aşağıdaki listelendiği üzere, çalışmalarımız sonucundaki proje çıktıları hedeflerimizin üzerinde gerçekleşmiştir.

- **Yayınlar:**
  - S. Gökçeli, M. Uslu, G.K.Kurt, B.Özbek, H. Alakoca, M.A. Durmaz, 'Implementation of Pre-FFT Beamforming in MIMO-OFDM',9th International Conference on Electrical and Electronics Engineering (ELECO),Bursa, Kasım 2015.
  - M.Uslu, H.B. Tuğrel, G.K.Kurt, B.Özbek, 'Yazılım Tabanlı Radyolarda Karşılıklı Kanal Özelliğinin İncelenmesi', 24. Sinyal İşleme ve İletişim Uygulamaları (SİU), Zonguldak, Mayıs 2016.

- Ö.Özdoğan, B.Özbek, G.K.Kurt, 'Güvenli çoklu kullanıcılı MISO sistemlerde eşik değerine dayalı kullanıcı seçim performansı', 24. Sinyal İşleme ve İletişim Uygulamaları (SİU), Zonguldak, Mayıs 2016.
- B.Özbek, Ö.Özdoğan, G.K.Kurt, 'Secure Multiuser MISO Communication Systems with Quantized Feedback', 27th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Workshop on Deployment perspectives of Physical Layer Security into wireless public RATs, İspanya, Eylül 2016.
- B.Özbek, Ö.Özdoğan, G.K.Kurt, 'Secure Multiuser MISO Communication Systems with Limited Feedback Link', Springer Annals of Telecommunications, Kasım 2016 (Hakem değerlendirmesinde).
- B.Özbek, G.K.Kurt, 'Spatial Signature for Secure MISO-OFDM Systems', IEEE Wireless Communications Letter, Kasım 2016 (Hakem değerlendirmesinde).
- O.A. Topal, G.K.Kurt, B. Özbek, 'Key Error Rate: A Theoretical Analysis and Measurement Results', IEEE Transaction on Vehicular Technology (Hazırlık aşamasında).
- B. Özbek, Ö.Özdoğan, G.K.Kurt, 'Secure Multiuser MIMO Communication Systems with imperfect channel state information', Wiley Transactions on Emerging Telecommunications Technologies (ETT) (Hazırlık aşamasında)
- Ö.Özdoğan, B.Özbek, G.K.Kurt, 'Zamanla ilintili kanallarda güvenli MISO sistemlerinin başarımı', 25. Sinyal İşleme ve İletişim Uygulamaları (SİU2017), Antalya (Hazırlık aşamasında).
- O.A. Topal, M.Uslu, G.K.Kurt, B.Özbek, 'Physical Layer Security Testbed: Channel Reciprocity and Key Error Rates in MIMO Channels', 14. International Symposium on Wireless Communication Systems (ISWCS), İtalya, (Hazırlık aşamasında).

- **Patentler:**
  - B. Özbek, G.K.Kurt, 'Frekans-Uzamsal İmzaya Dayalı Güvenli Çoklu Verici Antenli Kablosuz Haberleşme Sistemi', Türk Patent Enstitüsü. (Buluş bildirim formu hazırlandı (Başvuru aşamasında).

- **Tezler:**
  - Mert Eygi, 'Physical Layer Security in MISO and MIMO Systems', İYTE Elektronik ve Haberleşme Müh. Lisans Tezi, Haziran 2015.
  - Merve Uslu, 'Yazılım Tabanlı Radyolarda Fiziksel Katman Güvenlik Uygulamaları', İTÜ Elektronik ve Haberleşme Müh. Lisans Tezi, Haziran 2016.
  - Birsen Güler, 'Physical Layer Security in Multiuser MISO based Systems', İYTE Elektronik ve Haberleşme Müh. Lisans Tezi, Haziran 2016.
  - Ozan Alp Topal, 'Fiziksel Katman Güvenlik Sistemlerinde Anahtar Kestirimi ', İTU Elektronik ve Haberleşme Müh. Lisans Tezi, Haziran 2017 (Hazırlık aşamasında).

- Özgecan Özdoğan, 'Multiple antenna based phsyical layer security wireless systems' , İYTE Elektronik ve Haberleşme Müh. Yüksek Lisans Tezi, Haziran 2017 (Hazırlık aşamasında).

- **Sunumlar:**
  - B.Özbek, G.K.Kurt, O.A. Topal, 'Zaman uzamsal imzaya dayalı güvenli çok girişli çok çıkışlı kablosuz haberleşme sistemi', Airties A.Ş., Eylül 2016.
  - B.Özbek, G.K.Kurt, 'Zaman uzamsal imzaya dayalı güvenli çok girişli çok çıkışlı kablosuz haberleşme sistemi', Türk Telekom-Argela A.Ş., Eylül 2016.
  - M.Uslu, H.B. Tuğrel, G.K.Kurt, B.Özbek, 'Fiziksel Katman Güvenliğinde İmza Tabanlı Anahtar Çıkarımı', Aselsan Haberleşme Kurultayı, Kasım 2016.

2 Literatür Özeti

Telsiz ağların giderek yaygınlaşması, uygulama alanlarının çeşitliliği sebebiyle güvenlik problemlerinin önemini daha da arttırmaktadır. Veri iletişiminde taşınabilir (portable) ve mobil ağlar, askeri kullanımdan son kullanıcıya kadar ulaşmış, özel bilgi taşınması sebebiyle de güvenlik ihtiyacı kaçınılmaz olmuştur. Bu bölümde fiziksel katman güvenliğinde yapılmış olan çalışmalar ele alınmıştır. Fiziksel katmandaki güvenlik sistemi telsiz haberleşme kanalına bağlı özellikleri içerdiğinden kullanım yaygınlığı ve güvenlik ihtiyacının önemi göz önüne alınarak sistem yapısı olarak MIMO-OFDM seçilmiştir. MIMO-OFDM tabanlı sistemler, LTE, WiMAX gibi 3. Nesil (3G) hücresel haberleşme standartlarında, LTE-Advanced, WiMAX-Advanced gibi 4G hücresel haberleşme standartlarında ve IEEE 802.11n telsiz yerel alan ağı standartlarında olmak üzere, sağladığı avantajlardan ötürü günümüzde birçok telsiz haberleşme sisteminin temelini oluşturmaktadır.

2.1 Ağ Katman Güvenliği

Gizliliğin sağlanması için fiziksel katmandan farklı katmanlarda da çözümler geliştirilmiştir. Uygulama katmanında programlar arası veri paylaşımlarını önleyen mekanizmalar bulunmaktadır. Ağ katmanında sanal yerel alan ağları (Virtual Local Area Network; VLAN) gibi çözümler ile verilerin farklı ağlara gitmesi engellenebilmektedir. En önemli gizlilik önlemi, verilerin şifrelenmesi ile veri bağı katmanında sağlanmaktadır. Bu yöntemle, gönderilen mesajın yalnızca şifreleme anahtarına sahip alıcı tarafından çözülebilmesi sağlanmaktadır [1] - [10]. Bu sistemlerde anahtar gizliliği çok önemli olduğundan anahtar paylaşım aşaması kritik bir işlem olarak kabul edilmektedir.

Literatürde telsiz haberleşme kanallarında güvenli iletişimin sağlanması için geliştirilmiş temel teknikler veri bağı katmanında yapılan verinin şifrelenmesi ve yetkilendirme işlemlerini kapsar. Yetkilendirme, kullanıcının yetkili kullanıcı olarak kabul edilmesi anlamına gelir. Verinin şifrelenmesi ise, verinin yetkili olmayan kişiler tarafından ele geçirildiğinde anlaşılmasını engellemek için kullanılır. Şifreleme için alıcı ve verici tarafında şifreleme anahtarı bulunmalıdır. Birbirlerinden fiziksel olarak uzaktaki düğümlerin anahtar alışverişi aşamasındaki güvenlik oldukça kritiktir, çünkü anahtarı ele geçiren yetkisiz kişi daha sonra şifrelenecek tüm veriyi çözebilir.

Literatürde anahtar alışverişi problemine çözüm olarak birçok yöntem önerilmiştir. [54]'da Diffie Hellman yöntemi olarak bilinen asenkron anahtar paylaşımı yöntemi ile çözüm getirilmiştir. Bu yöntem ile özel anahtarlar gönderici ile alıcı arasındaki hattan gönderilmeksizin, iki tarafta da aynı şifreleme anahtarı elde edilmektedir. Ancak bu işlem sırasında eğer özel anahtarlar uzun seçilmezse gizli dinleyiciler deneme yoluyla özel anahtarları bulabilir. Bu sebeple anahtarlar mümkün oldukça uzun seçilmelidir. Bu anahtarın, başka kimsenin ele geçiremeyeceği şekilde iki taraf arasında paylaşılması çok önemlidir, çünkü anahtar paylaşımı sırasında anahtarı ele geçiren kişiler tüm şifrelenmiş iletişimi çözme yetisine sahip olurlar. Bu yüzden, anahtar paylaşımı işlemi sırasında kullanılan hesaplama karmaşıklığı veri şifrelemesinden çok daha yüksek tutulur. Bu durumda, cihazlarda yüksek karmaşıklığa sahip hesaplamanın yapılması için yeterli işlemci gücünün sağlanması zorunluluğu ortaya çıkar. Taşınabilir cihazlardaki

pil ömrü de bu işlem yükünden olumsuz şekilde etkilenir. İşlem yükünün azaltılması hem uygulama zorluğunun aşılması, hem de kullanım süresinin artması açısından olumlu etki yaratacaktır.

2.2 Fiziksel Katman Güvenliği

Telsiz ağlarda fiziksel katmanda yapılan güvenlik saldırıları pasif ve aktif saldırılar olmak üzere iki sınıfta incelenebilir [11]. Aktif saldırı tiplerinde saldıran taraftan servis sağlayıcıya bir etkide bulunulur. Bu etki sayesinde aktif saldırıları yakalayan saldırı tespit sistemleri (intrusion detection systems; IDS), saldırıyı bitirecek şekilde önlemler alırlar. IDS sistemleri günümüzde yaygın olarak kullanılmaktadır. Ancak, pasif saldırılar servis tarafında algılanamadığı için IDS tarafından engellenemezler. Pasif bir saldırı tipi olan gizli dinleyici saldırıları (eavesdropping attacks), verici ile yetkili alıcı arasındaki trafiğin yetkili olmayan alıcılar tarafından ele geçirilerek verinin çözülmesi olarak tanımlanır. Trafik analizi saldırıları da gizli dinleyici saldırılarının özel bir türüdür ve verinin içeriğinin çözülmediği durumda bile trafiğin ele geçirilip analiz edilmesi yoluyla özel bilgi edinilmesi anlamına gelir. Pasif saldırılara karşı iletişimi koruma altına almak, başka bir deyişle gizliliği (secrecy) sağlamak gerekmektedir. Bunun yanında kablolu sistemlerden farklı olarak telsiz haberleşme sistemlerinde iletim ortamı herkese açıktır. Herhangi bir önlem alınmadığı takdirde verici anteninin kapsama alanı içindeki bütün alıcı düğümler veriyi ele geçirebilir [12]. Bu durum gizliliği tehlikeye atan büyük bir problemdir ve günümüzde yapılan fiziksel katman güvenlik çalışmalarının ana amacı bu gizlilik açığını kapatarak telsiz haberleşme sistemlerini daha güvenli hale getirmektir [13] - [15].

Fiziksel katmanda güvenlik, kablosuz haberleşmenin yaygınlaşması ile önem kazanmış bir kavramdır. Fiziksel katmanda güvenlik konusunda yapılmış olan çalışmaların büyük bir kısmı [16] çalışmasına dayanmaktadır. 1975 yılında yayınlanmış bu çalışmada Wyner ilk kez dinlenen kanal (wiretap channel) kavramını kullanmıştır. Bu kavram, gizli dinleyici kanalının, yetkili alıcı düğüme ait kanalın daha yüksek gürültülü bir versiyonu olduğu özel bir durumu tanımlamaktadır. Wyner bu çalışmasıyla daha önce yapılmış olan şifreleme yöntemlerinin ulaşamadığı gizlilik oranının (secrecy rate) fiziksel katman yaklaşımında ulaşılabildiğini kanıtlamıştır. 1978 yılında yayınlanmış [17]'deki çalışmada ise, gizli dinleyici genelleştirilerek yetkili alıcının kötüleştirilmiş bir hali yerine bağımsız bir kanal modeli kullanılmıştır. Ancak, yine de bir mesajı yetkili alıcıya güvenli iletebilmek için gizli dinleyici kanalının yetkili alıcı kanalına göre daha gürültülü olması gerektiğini öne sürülmüştür. Bunu takip eden çalışmalarda, öncelikle bilgi kuramı yaklaşımları kullanılmış, "güvenli kanal kapasitesi (secret channel capacity)" tanımı ortaya atılarak bu kapasitenin sınır değerlerinin bulunması ve arttırılması hedeflenmiştir. Güvenli kanal kapasitesi, yetkili alıcı düğümünün kanal kapasitesi ile gizli dinleyicinin entropileri arasındaki farka eşit olarak tanımlanmıştır. MIMO sistemlere de uygulanmıştır [13], [18] - [20]. Önerilmiş bu modellerden yola çıkılarak farklı senaryolar üzerinde bu modelin uygulanmasına yönelik çalışmalar yapılmıştır [21] - [24]. Bilgi kuramı yaklaşımı ile güvenlik uygulamaları ortalama bir ölçütte çalışmaktadırlar ve kanalın mükemmel bilindiği varsayımına dayanmaktadır ki, bu da pratikte her zaman mümkün değildir.

2.3 Çoklu Antenli Sistemlerde Fiziksel Katman Güvenliği

Çoklu anten dizilerinin kullanımı ve hüzme yönlendirme yöntemleri ile güvenlik seviyesi arttırılabilmektedir. İlk hüzme yönlendirme çalışmaları, işaret boğma saldırılarını önlemek üzerine [25]'de ele alınmıştır. Bu çalışmada yönlü anten kullanımında, yönsüz (omnidirectional) anten kullanımına göre daha yüksek başarım elde edildiği gösterilmiştir. Daha sonra [26]'da yapay gürültünün eklenmesinin sistem güvenliğine etkileri incelenmiş ve maksimum güvenliğin bu şekilde garantilenebileceği belirtilmiştir. Bu yaklaşımda yapay gürültü, yetkili alıcının dışındaki uzaya gönderilmekte ve yetkili alıcı bu gürültüden etkilenmemektedir. Bu durumda yeterli çıkış gücü kullanılırsa gizli dinleyicinin kanalı, yetkili alıcının kanalından daha iyi olsa bile güvenlik sağlanabilmektedir. [27]'de akıllı gürültü yöntemleri geliştirilerek belirli SINR değerini garantileyen ya da çıkış gücünü sınırlayan optimizasyon problemleri önerilmiş ve farklı sistem senaryolarında başarımlar incelenmiştir. [28]'de LTE standardında kullanılan hücreler arası girişimi önleyen hüzmeleme matris indekslerine dayalı fiziksel katman güvenlik yöntemi verilmiştir.

[29]'da tek girişli çok çıkışlı (single input multiple output, SIMO) sistemler için güvenlilik çeşitlilik kazancının (secrecy diversity gain) alıcı anten sayısı ile orantısal bağıntılı olduğu görülmüştür. Buna karşılık düşen çok girişli tek çıkışlı (multiple input single output, MISO) kanallardaki güvenli kanal kapasitesi [30] ve [31] çalışmalarında incelenmiştir. Bu çalışmaların ardından MIMO sistemlerde güvenlik çalışmaları hız kazanmıştır [26], [32]- [36]. [32]'de iki antenli alıcı ve verici ile tek antenli gizli dinleyicinin olduğu durumda optimum sonuç veren bir hüzme yönledirme yöntemi önerilmiştir. Verici ve gizli dinleyici düğümlerinde çoklu anten olan kanallara MISOME; alıcı, verici ve gizli dinleyici düğümlerinin her birinde çoklu anten olan kanallara MIMOME ismi verilmiş ve [36] ile [13]'de ayrıntılı bir şekilde ele alınmıştır. Sonrasında MISO kanallarda [37] - [39] ve MIMO kanallarda [37] ve [40] çalışmaları yapılmıştır. [41] - [43]'de MIMO-OFDM sistemler üzerinde fiziksel katman güvenliği yöntemleri incelenmiştir.

[44]'de tüm kanal durum bilgisinin (channel state information; CSI) elde edilebildiği durum ele alınmış, bu koşul altındaki güvenlik kapasitesi, yalnızca yetkili alıcının CSI'nın verici tarafından bilindiği durum için üst sınır olarak belirlenmiştir. [30]'da ise SIMO sistemler ele alınmıştır. Renkli gürültülü SIMO kanalı, skalar Gauss dinlenen kanala dönüştürerek öncesinde önerilmiş olan tekniklerle güvenlik kapasitesinin hesaplanmasının sonucunda, birden fazla anten kullanımının sistem başarımını arttıracağı görülmüştür.

Mevcut hüzme yönlendirme yöntemlerinin kanal kestirim hatalarına karşı olan duyarlılığı [45]'de incelenmiş ve sistemin bu hatalara karşı oldukça duyarlı olduğu gösterilmiştir. Bu tip hatalara karşı önlem alınmadığı sürece, mevcut yöntemlerin başarımları hızlı bir şekilde düşmekte ve pratikte uygulanabilirliği azalmaktadır.

Gizli dinleyicinin kanal bilgisi de fiziksel katman güvenliği açısından oldukça önemli bir noktadır. Çalışmaların çok büyük bir bölümünde [26], [29] - [35], verici ile gizli dinleyici arasındaki kanal bilgisinin tam olarak bilindiği varsayılmıştır. Ancak bu varsayımın pratikte gerçeklemesi zordur, çünkü gizli dinleyici saldırıları çoğunlukla pasif saldırı türüdür ve sistemin gizli dinleyicinin bilgisini elde etmesi mümkün değildir. Bunun yanı sıra, gizli dinleyici hakkında istatistiksel bazı kanal özelliklerini bilmek de mümkün olabilir. [39] ve [46]'da kısmi kanal bilgisine sahip olunduğu durumdaki sistemler ele alınmıştır. Gecikmeli kanal bilgisi durumu [47] ve yal-

nızca yön bilgisinin bilindiği durum [48]'de incelenmiştir. Kanal ile ilgili hiçbir bilginin bilinmediği durum ise [49] - [51] çalışmalarında ele alınmıştır.

2.4 Kanal Durum Bilgisini Kullanarak Anahtar Üretilmesi

[52]'de bahsedildiği gibi, iletim hatlarındaki veri güvenliği için devam eden şu anki araştırmalar temelde üç başlık altında toplanabilir. Bunlardan birincisi kriptografi temelli uygulama katmanında araştırılan güvenlik önlemleri, ikincisi Shannon'ın [53]'da temelini attığı sonrasında da Wyner [16], Czizszar & Körner [17] gibi isimlerin devam ettirdiği bilgi kuramı temelli fiziksel katmanda güvenlik çalışmaları, en son olarak da daha yakın dönemde ortaya çıkmış kablosuz iletişim kanalının özellikleri kullanılarak fiziksel katmandaki güvenlik araştırmalarıdır.

Temel kriptografi sistemlerinde, mesajı (plaintext) şifreleme ve şifre çözme yöntemlerinde kullanılacak anahtarı paylaşma biçimleri, gizli anahtar (secret key) ve açık anahtar (public key) olarak sınıflandırılır. Gizli anahtar paylaşımında, A (Alice) ve B (Bob) arasındaki haberleşme önceden belirlenmiş bir anahtar (ya da anahtarlar dizisi) kullanarak yapılır. Ancak bu tip bir sistemde, eğer A ve B daha önce hiç yan yana bulunmadıysa ya da aralarında güvenli bir iletim hattı yoksa anahtar paylaşımı sorunu ortaya çıkar. Bu sebepten ötürü herkese açık anahtarlar üretilip paylaşılmış ve anahtar paylaşma sorunu çözülmüştür. Şu anda en sık kullanılan herkese açık anahtar paylaşma algoritmaları Diffie Hellman [54] ve RSA'dir. Bu mevcut tasarımlarda kullanılan kriptografi tabanlı güvenlik sistemleri, hesaplamaya dayalı olduklarından, iyi bir güvenlik sağlamaları için yüksek güç tüketmeleri gerekir ve dolayısıyla sensör ağlar, mobil cihazlar gibi alanlarda kullanıldığında bu sistemler verimsizleşirler. Bilgi kuramı temelli çalışmalar, sağlanabilecek gizlilik kapasitesi hakkında üst sınır verse de, iki kullanıcı arasında güvenli bir kanal olması varsayımı altında geçerlidir [55]. Bu durumda da eğer bir güvenli kanal varsa bu kanaldan herhangi bir anahtar paylaşımı yapılacağı için bu varsayım gerçekçi değildir. Bu sebeplerden ötürü fiziksel katmandan edilecek bilgiye dayalı kriptografik anahtar üretme araştırmaları hız kazanmıştır. Bu tarz yöntemlerde iletişimin her iki yanında, kablosuz kanalların bazı temel özellikleri kullanılarak gizli anahtarlar üretilir ve üretilen bu anahtarların birbirine uyuşması isterir. Aşağıda kablosuz kanal özellikleri kullanım amaçlarıyla ilişkili olarak açıklanmıştır [56], [57].

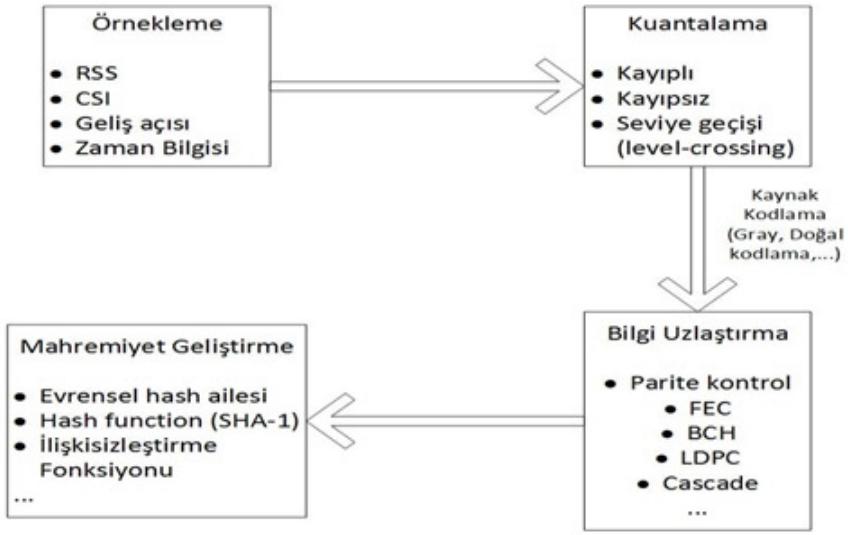
- Elektromanyetik Dalgaların Karşılıklı Olması (Reciprocity): Çok yollu kanallardaki kazançlar, faz ötelemeleri ve gecikmeler, iletişimin her iki taraftında da aynı olduğu durumdur. Bu özellik alınan işaret gücünün (RSS) her iki tarafta da aynı olmasını garanti etmez, RSS asimetrik olabilir. Bu özellik kullanılarak, her iki kullanıcı yaptığı ölçümlerle karşılıklı aynı kanal parametreleri kullanarak bir anahtar üretebilir.

- Kanaldaki anlık değişimler: Kullanıcıların her türlü konum, açı, vb. değişimleri kanal özelliklerini anlık olarak değiştirir.

- Uzaysal çeşitlilik: Kullanıcılar ve gizli dinleyici arasındaki uzaklık bir kaç dalgaboyundaysa, kullanıcılar ve gizli dinleyiciye ait kanalların özellikleri ilişkisizdir.

2.4.1 Temel Prensipler

İlk olarak [55]'de belirtilen, sonrasında [56] - [59] gibi birçok çalışmada fiziksel katmanda anahtar dört temel adımda üretilir ve süreç Şekil 3'de verilmiştir. Literatürdeki yayınlarda gerçekleşen çeşitlilikler de, genel anlamda bu dört aşamadaki işlemlerin farklı yaklaşımlarla tamamlanmasıyla ortaya çıkar. Şekilde de gözüktüğü üzere ilk olarak, her iki kullanıcı arasındaki bir kanal parametresinin ölçülmesiyle elde edilen veriler her iki tarafta da kaydedilir. Bu ölçümler kanal katsayıları, RSS değerleri gibi çeşitlendirilebilir. Anahtar üretme yöntemleri, seçilen ölçüm değişkenine göre bir sınıflandırma sunar. Ölçümler esnasında dikkat edilmesi gereken önemli bir nokta ise, her iki kullanıcı tarafından aynı anda ölçümlerin yapılamamasından dolayı, iki ölçüm arasındaki sürenin olabildiğince kısa tutulmasıdır [56] - [61]. Çünkü aradaki zaman farkı arttıkça elde edilen ölçüm değerleri kanalın rastgeleliğinden dolayı farklılaşmaktadır.



Şekil 3: Fiziksel katmanda anahtar üretmek için temel aşamalar

İkinci adım olarak elde edilen ölçüm verisinin analog bir değer olması sebebiyle, bu verinin nicemleme işlemi gerçekleştirilir. Yine bu aşamada, nicemleme işlemi çeşitlendirilebilir. [56]'da RSS ölçümleri (ya da işaretin zarfı) için kayıplı ve kayıpsız nicemleme gerçekleştirilmiş ve [62] - [65]'daki nicemleme yöntemiyle karşılaştırılmıştır. Şu ana kadar anlatılan iki aşama da, her iki kullanıcı tarafında da yapılmalıdır. Bu esnada elde edilen iki nicemlenmiş bit dizisi karşılaştırılacak olursa, gürültü, girişim, donanım farklılıkları gibi sebeplerden ötürü elde edilen iki anahtar arasında bir asimetriklik gözlenir. Bu farklılıkların giderilmesi için kuantum kriptofrafi temelli iki aşama daha eklenir; bunlar bilgi uzlaştırma (information reconciliation) ve mahremiyet genişletme (privacy amplification) adımlarıdır [65].

Üçüncü adım olan Bilgi Uzlaştırma (Information Reconciliation) işleminde ise, kullanıcılardan biri diğerine kendi bit dizisi hakkındaki bilgiyi dışarıya çok fazla açıklamadan iletmelidir. Bu aşamada önemli bir yöntem Cascade metodudur [56] ve bu yöntemde örneğin A kullanıcısı kendi bit dizisinin sırasını rastgele değiştirir (permutation) ve sonra küçük bloklara böler. Ardından bu blokları ve denklik bilgisini B'ye gönderir. B de aynı işlemi kendi kuantalanmış bit dizisi için yapar ve A'dan gelen bilgiyle karşılaştırır. Eğer bu iki işlem sonucunda yakın ama farklı

sonuçlar elde edilirse, B parite bilgisine uyacak sonucu ikili arama (binary search) ile bulabilir. Bu işlem belli bir sayıda tekrar edilir ve hata olasılığının belli bir eşik değerinin üstüne çıkması istenir [66]. Bu Cascade yöntemi dışında, bir taraf LDPC [59], [67], [68], BCH [60] gibi kodlama algoritmaları kullanılarak elde edilen sendromu diğer tarafa gönderir ve diğer kullanıcı da kendi kuantalanmış verisini ve bu sendromu kullanarak yeni bir anahtara karar verir. Bir diğer yöntem olan belirsiz (fuzzy) bilgi uyumlaştırma kullanılarak anahtar üretme tekniğidir [65], [69].

Son olarak mahremiyet genişletme adımında ise elde edilen anahtar bit dizilerini birbirinden ilişkisiz hale getirmektir. Fiziksel şartlar gereği birbiriyle ilişkili olan ölçüm sonuçlarından elde edilen anahtar bitleri de birbiriyle ilişkili olur ancak, gizli dinleyici anahtarın bir kısmına erişse bile tüm anahtar dizisini çözmemelidir [56]. Bu aşamada doğrusal eşleştirme [59], hash fonksiyonları [56], [60], [65], [70] ve extractor kullanılabilir.

[57]'da özet olarak anahtar üretme aşamalarında ortaya çıkan problemler şu şekilde sıralanmıştır : 1) Eş zamanlı olmayan ölçümler 2) İlişkili bit dizileri ve 3) Düşük bit hızlı anahtar üretimi. Yine bu çalışmada, bu yöntem kullanılmadan, üç adımdan oluşan yeni bir tasarım kullanılarak anahtar üretimi yapılmıştır. Bu adımlar şu şekilde sıralanabilir: 1) Kısmi İnterpolasyon 2) İlişkisizleştirme dönüşümü 3) Çok bit uyarlamalı nicemleme (MAQ). [59]'da ise Gauss kaynaklar kullanılarak anahtar üretimi yapılmıştır. Bu aşamada evrensel bir bilgi uyumlaştırma yöntemi önerilmiştir.

2.4.2 Anahtar Üretme Yöntemleri

İki kullanıcı arasındaki kanal üzerinden farklı parametrelerin ölçülmesine bağlı olarak, anahtar üretme işlemi çeşitlendirilebilir. Bu yöntemlerden sırasıyla kanal bilgisi, RSS ve zaman bilgisi tabanlı anahtar üretmeye yönelik çalışmalar irdelenecek ve sonrasında OFDM ve MIMO sistemlere dair yapılan çalışmalardan bahsedilecektir. Birçok çalışma içerisinde de anahtar üretme yöntemleri tasarlanırken, gizli dinleyiciye de ait bir model oluşturulmuştur [56], [57], [71], [72]. İlaveten, çoklu antenli, farklı frekanslarda ölçüm yapan, ve kablosuz kanaldaki varyansyonları kullanan sistemlerde, tek RSS ölçüm ya da tek frenkastaki herhangi bir ölçüme dayalı sistemlere göre daha güçlü anahtar üretildiği belirtilmiştir [73].

Kanal Bilgisinin Kullanılması: [62]'de sistemin kanal katsayıları seviye geçişi algoritması (level-crossing algorithm) kullanılarak bulunmuş ve bu katsayılara dayalı anahtar üretme işlemi yapılmış, sistemin başarımı kanalın darbe cevabı (CIR) ve RSSI yaklaşımlarıyla incelenmiştir. [72]'da ise kanalın karşılıklı olması (reciprocity) kullanıcıların doğruluğunu tespit etmek için kullanılırken (authentication), CSI dayalı anahtar üretme çalışmaları yapılmıştır. Bu çalışmanın bir diğer önemli özelliği, yazılım tabanlı radyo (SDR) altyapısına sahip USRP ve GNU kullanılarak testler gerçekleştirilmiştir. [74]'de ise Gauss kaynaklar için CSI bilgisi anahtar üretmek için kullanılmıştır. Bunların yanında kanalın faz bilgisini kullanan yayınlar da mevcuttur. Bu çalışmaların en temelinde olan araştırmalarda [75] - [77] kanalın zamanda çok kısa bir an için sabit kaldığını ve bu sürede reciprocity özelliği altında faz farkı kullanılarak anahtar üretme işlemleri incelenmiştir. [52]'de doğrudan faz kuantalanarak gizli anahtar üretilmiştir. Bu çalışmada eğer anahtarlar eşleşmez ise, aynı işlem eş anahtarlar bulununcaya kadar devam ettirilmekte-

dir. [61]'de ise sistem optimizasyonu için faz bilgisinin kuantalanması sırasında koruyucu aralıklar (guard interval) ya da faz ötelemesi yöntemleri kullanılmıştır. Bu çalışmada çok yollu kanallar için, gecikmelerle farklı yollardan elde edilen kanal cevaplarının birbirinden bağımsız olduğu ve ayrı ayrı kuantalanabileceğinin üstünde durulmuştur. Düzgün dağılmış faz bilgisi kullanılarak elde edilen anahtar üretilmesinin RSS tabanlı anahtar üretme yöntemlerine göre avantajları sıralanmıştır [71]. Bu avantajlar arasında, ikili yerine grup anahtar üretimi, yüksek gizli bit hızı, yüksek entropi ve hareketli veya sabit durumda anahtar üretebilme özellikleri sıralanmıştır.

RSSI tabanlı en kapsamlı çalışmalardan biri olana [56]'da farklı bir nicemleme tekniği önerilmiş ve bu teknik diğerleriyle karşılaştırılmıştır. Bu çalışmada RSSI temelli yöntemlerin seçilmesinin nedeni, kullanılan birçok kablosuz sistemde herhangi bir değişiklik yapmadan kolayca ölçümlerin yapılması olarak gösterilmiştir. Bu çalışmada gerçek ortamlarda testler yapılmış ve gösterilmiş ki, sabit ortamlarda karar verilen anahtarlar daha güvensiz olurken, hareketli durumda elde edilen anahtar dizisi daha güvenli olmuştur. Hüzme yönlendirme kullanarak RSSI ölçümlerine dayanan anahtar üretme yöntemi ise [64]'de sunulmuştur. [78]'de ise yıldız ve zincir şeklindeki bir ağ durumunda çok kullanıcı için RSSI ölçümleri yapılarak anahtar üretilmek istenmiştir ve bu durumda röle görevini üstlenen kullanıcıların etkisi gözlenmiştir. Önceki bölüm içerisinde de belirtildiği [57]'da RSSI temelli anahtar üretmiş ancak standart prosedür yerine yeni bir prosedür önererek literatüre katkıda bulunmuştur. [65]'de ise elde edilen işaret zarf değerlerindeki ani düşüşler (deep fades) kullanılmıştır. Bu değer belli bir eşik değerinin altına düşmesi durumunda 1 olarak kodlanır, diğer durumlarda ise 0 olarak kodlanır. Güvenlik anahtarının alınan işaretin gücünden RSS ölçümlerinden elde edilmesi ve gerçek test ortamında başarım sonuçları [79]'de elde edilmiştir. Kanalın durağan olduğu durumlarda üretilen anahtarın veri hızının çok düşük olduğu fakat dinamik kablosuz kanal durumunda bu veri hızının çok daha yüksek olduğu gözlemlenmiştir. [80]'da RSSI tabanlı anahtar üretme algoritması olan ARUBE (Adaptive Ranking based Uncorrelated Bit Extraction)'nin tasarımı yapılmış ve bu algoritmada kanaldaki gürültü ve girişimden kaynaklı eşleştirilememe (non-reciprocity) sorunlarını dört aşamada aşılmıştır: interpolasyon, sıralama (ranking), ilişkisizleştirme (decorrelation) ve nicemlemedir.

RSS ölçümleri yapılarak yapılan anahtar üretme işlemlerinin en önemli avantajı, mevcut sistemler üzerinden kolayca ve ucuz biçimde gerçeklenebilir. RSS tabanlı yöntemlerin dezavantajları ise [71]'de açıkca belirtilmiştir ve şu şekilde listelenebilir:

- Anahtar biti üretme hızı oldukça düşüktür.
- Çok kullanıcı durumda çoklu anahtar üretmesi kolay değildir.
- Anahtar üretme işlemi kanal varyasyonuna dayandığından, durağan kullanıcılar için uygun değildir.

2.4.3 OFDM ve MIMO Sistemlerdeki Yaklaşımlar

Bu projede temel haberleşme altyapısı MIMO ve OFDM sistemler üzerine kurulmuştur ve literatürde bu sistemleri ayrı ayrı ya da ortak olarak içeren anahtar üretme çalışmaları bu başlık altında verilecektir. MIMO sistemlerinde güvenlik anahtarının üretimi [81]'de yapılmıştır ve

iç mekan kablosuz ortam testleri gerçekleştirilmiştir [73]. Alıcı ve verici arasındaki kablosuz kanalın zamanda değişmediği özelliğinden faydalanarak çoklu anten uygulamalarında güvenlik anahtarındaki bit sayısı için üst limit elde edilmiş ve bu limite sönümlemeli kanallarda erişmek için algoritma tasarımı yapılmıştır [82]. Önceki kısımlarda bahsedilen çalışmalar arasında yer alan [52], [61]'de OFDM kanal katsayılarının faz bilgileri kullanılarak anahtar üretme yoluna gidilmiştir. [83] ve [68]'da ise, OFDM kanal katsayıları kullanarak anahtar üretmenin, RSSI temelli yönteme göre daha iyi gizli anahtar kapasitesi sağladığı gösterilmiştir. Bu çalışmalarda anahtar üretme problemi bir Slepian-Wolf kodlama ve kod çözme problemi olarak düşünülmüş, farklı tipteki LDPC kodlar bilgi uyumlaştırma aşamasında kullanılmıştır. Burada örneklenmiş ölçümler kuantalanmış veya kuantalanmamış biçimde diğer kullanıcıya gönderilip, bu senaryolar ayrı ayrı incelenmiştir. [73]'de OFDM sistemindeki CSI kullanılarak anahtar üretme yöntemi tercih edilmiş ve kapalı/açık alanda hareketli/sabit senaryolar için gerçeklemeler yapılmıştır.

Çok antenli durum için ise, [84], [85]'da CSI bilgisini kullanıp kanal nicemleme yöntemleriyle anahtar üretimi gerçekleştirmişlerdir. [85]'da MIMO durumu için yapılan anahtar üretme çalışmaları, kapalı ortam için genişband durumunda gerçeklenmiştir. [81]'da ise RSSI temelli anahtar üretme yöntemi MIMO durum için genişletilmiştir. Bu çalışmada elde edilen deneysel sonuçlara göre, çoklu anten kullanmak tek antenli duruma göre daha hızlı gizli bit üretimi sağlar. Ayrıca, çok düzeyli nicemleme da ikili nicemlemeye göre daha hızlı bit üretimine yardımcı olur. Hem yüksek hem de düşük güç bölgelerinde güvenli-anahtar kapasitesi durağan sönümlemeli MIMO kanallar için [86]'de üretilmiştir. Fakat bu çalışma hem alıcı hem verici hem de gizli dinleyici tarafından tüm kanal katsayılarının bilindiği varsayımına dayanmaktadır. [87], [88]'da ise uzamsal ilişkinin Kronecker olarak modellendiği MIMO durumlar için, ön kodlama ve uzamsal ilişkinin farklı SNR'larda anahtar üretimine etkisi incelenmiştir. Bu sonuçlar göstermektedir ki, düşük SNR'da uzamsal ilişki anahtar üretme hızını arttırmaktadır. Diğer yandan, yüksek SNR'da maksimum anahtar üretme hızına ilişkisiz antenler kullanılarak erişilmektedir. Bunların yanında optimum ön kodlama işlemleri de incelenmiştir. [89]'de ise, yine Kronecker ilişki modelinde, MIMOME sistemlerde Rayleigh sönümlemesi altında erişilebilir anahtar hızının alt ve üst sınırları için kapalı form ifadeleri bulunmuştur. Ek olarak, bu koşullar altındaki optimum pilot işaret kümesi araştırılmıştır. [90]'de ise MIMO sistemler için anahtar üretme mekanizması matematiksel olarak açıklanmış, devamında ise işbirlikli MIMO sistemler için güç paylaşımlı (power allocation) anahtar üretme yöntemleri önerilmiştir. Bu çalışma MIMO sistemler için anahtar üretme yöntemlerini detaylı bir şekilde açıklanmasıyla öne çıkmaktadır. [79]'da ise, MIMO tipi sensör test ortamında ölçümler yapılmıştır. Sonuçlara göre, MIMO sistemler için RSSI tabanlı anahtar üretme yönteminde SISO'ya göre yüksek hatalı bitle karşılaşılmıştır. Bu sorunun çözümü için, damıtma aşaması (distillation stage) isimli bir yöntem geliştirmişlerdir. Bu yönteme göre, nicemlemeden sonra hatalı bitlere sebep olacak değer bulunarak silinir.

2.4.4 Performans Metrikleri

[58]'da temel performans incelemeleri için gereken çıktılar olarak anahtar eşleştirme oranı, gizli bit üretim hızı, entropi, gerçekleme karmaşıklığı ve önekler gösterilmiştir. Bunların yanında [56]'da NIST testinden bahsedilmiştir ve bu test üretilen anahtar bit dizisinin rastlantısallığını

ölçmektedir [91]. [62]'de anahtar eşleştirme oranı, gizli bit üretim hızı ve bitler arasındaki ilişki (NIST testi kapsamında) için detay bir şekilde incelenmiştir. [57]'da bitler arasındaki ilişki katsayısı iki farklı yöntemle ölçülmüştür; 1) İkili (Pair-wise) bit ilişki katsayısı 2) Küresel bit ilişki katsayısı. Genel anlamda bu sistemlerde gecikme, hesap karmaşıklığı ve ilişki arasında bir ödünleşim (tradeoff) gözlenir. Bu yüzden sistem incelemeleri bu durumlar göz önüne alınarak yapılmalıdır. Bir başka performans kriteri de, gizli dinleyicinin diğer kullanıcılarla aynı anahtarı üretme olasılığıdır ve bu olasılık [76]'da olasılıksal gizlilik (probabilistic secrecy) olarak tanıtılmıştır.

2.5 Fiziksel Katman Güvenliğinden Yazılım Tabanlı Radyo

Yazılım tabanlı radyo, özelleşmiş bir alıcı ve verici donanımı yerine yazılımla kontrol edilebilen genel bir alıcı/verici içeren donanım ve bunu kontrol etmek için bir yazılımın kullanımıyla elde edilen radyo çeşididir. Bu genel bir tanım olup, bir yazılım tabanlı radyo sistemini gerçeklemek için hem donanım hem de yazılım tarafında çeşitli çözümler bulunmaktadır. Bu çözümlerden literatürde en sık kullanılanı Universal Software Radio Peripheral (USRP) kitleridir [92]. USRP kitleri, bir bilgisayara bağlanabilen ve bilgisayar üzerinden yazılımla kontrol edilebilen bir radyo düzeneği olup, proje kapsamına kullanımı yapılmıştır. USRP kitleri, yazılım tabanlı radyo için yapılmış olan diğer donanımlardan MATLAB programı ile uyumlu olması ve uygulama çeşitliliği bakımından ayrılmaktadır. Yazılım tabanlı radyolarda MIMO sistemlerin gerçeklemeleri [93] - [95] ve OFDM sistemi gerçeklemesi [96] - [100] çalışmalarında yapılmıştır. [101]'de ise, USRP'lerden oluşan bir düzenek hazırlanmış ve kanal kazancı kullanılarak bu sistem için anahtar üretimi yapılmıştır.

2.6 İlgili Patentler

Telsiz haberleşme kanalından gizli iletişimi sağlayacak anahtarın oluşturulması konusunda bir Amerikan Patent Ofisi patenti bulunmaktadır [102]. Bu çalışmada pratikte kullanılabilecek şekilde güvenlik sistemlerini kod-kitapçığı tabanlı yaklaşım bulunmamaktadır.

Güvenli kanalın seçimi ve hüzme oluşturma tabanlı fiziksel katmana bağlı olarak veri iletişim güvenliğini arttıran [103] ve yapay gürültü kullanarak iletişimin gizliliğini sağlayacak bir sistem öneren [104] patentler vardır. Bu sistemlerden hiçbiri MISO-OFDM sistemlere yönelik olarak pratikte de kullanıma uygun olacak şekilde MISO kanalların frekans-uzamsal imzalarını kullanarak kod kitapçığı tasarlamaya yönelik değildir.

MISO sistemlerde kod kitapçığı kullanımı bilinen bir yaklaşımdır [105], [106]. Kod kitapçığı kullanımı çok hücreli yapılarda da mümkündür [107]. Kod kitapçığı kullanarak fiziksel katman sistemlerde güvenliğin sağlanabildiği de bilinmektedir [108] [110]. Bu çalışmalar ele alınan yaklaşımı doğrulamaktadır. Bununla beraber mevcut sistemlerde OFDM/OFDMA tabanlı frekans çeşitliliği kullanılarak alt-taşıyıcı kümeleme ve kod kitapçığını açısal olarak odaklama teknikleri önerilmemiştir. Açısal olarak ele alınan eşit-olmayacak şekilde bölünme yaklaşımı konusunda bir patent bulunmakla beraber bu yaklaşımın sistem güvenliğini artırmak için kullanılmamış olduğu görülmektedir [111].

Benzer bir patent ya da patent başvurusu TPE kayıtlarında bulunamamıştır. En yakın olarak değerlendirilebilecek patentler fiziksel güvenlik içermekte olup sistem bileşenlerinin güvenli bir kabinde konumlandırılması prensibine dayanmaktadır [112], [113]. Bu çalışmalar fiziksel katman güvenliği ile bağlantılı değildir.

[114] 'de baz istasyonları arasında hüzmeleme kod kitapçığı alışverişini sağlayan bir sistem ve yöntemden bahsedilmektedir. Fakat bu buluşta, rastgele üretilen vektörlere göre kümelenmiş alttaşıyıcıların sınıflandırılması ve bu sınıflandırmaya baz olan vektörlere göre döndürülmüş kod kitapçıklarının oluşturulmasından bahsedilmemektedir. [115]'de ise bir iletişim sisteminden bahsedilmektedir. Bu sistemde pilot sembollerle kanal kestirimi yapıldığından, bir önkodlama matrisi kullanan bir önkodlama biriminde, alt taşıyıcıların sınıflandırılmasından ve rastgele fazların oluşturulmasından bahsedilmektedir.

[116]'de pilot sinyal ile kanal kestirimi yapılmasından ve alt taşıyıcı kümelerinin sınıflandırılmasından bahsedilmektedir. Ancak bu buluşta kümelenmiş alt taşıyıcıların sınıflandırılması ve bu sınıflandırmaya baz olan vektörlere göre ayrı kod kitapçıklarının oluşturulmasından bahsedilmemektedir.

3 Gereç ve Yöntem

3.1 MIMO

Kablosuz haberleşmede iletişimin hızının artması, ana hedef haline gelmiştir. Frekans spektrumunun azlığına rağmen bilgi iletiminin yüksek hızlarda sağlanma ihtiyacı, kablosuz iletişimde spektral verimliliği ve kaliteyi artırma, etkin kodlama ve modülasyon tekniklerine gereksinimi doğurmuştur.

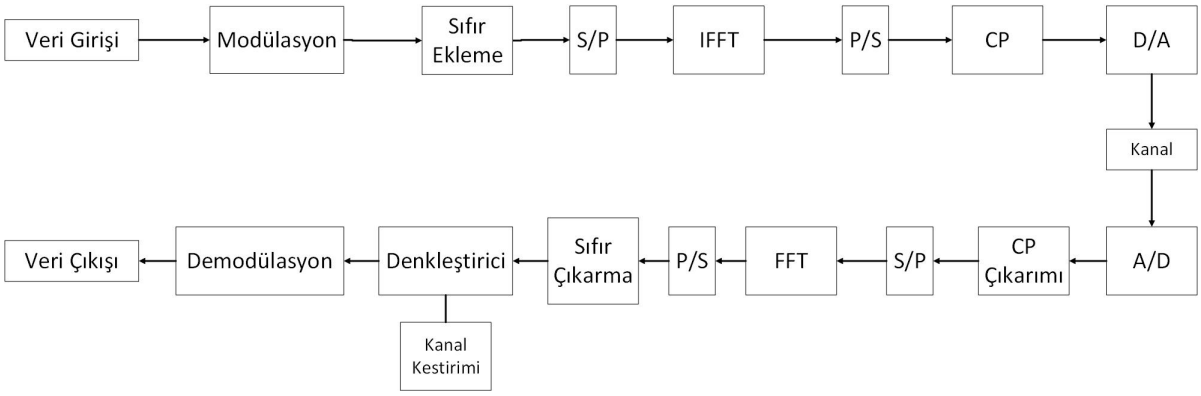
Çoklu-yoldan gelen sinyallerin alıcıdaki toplamı alınan sinyalin gücünde dalgalanmalara sebep olur. Bu dalgalanmalar sönümleme olarak adlandırılır. Bu yüzden vericide ve alıcıda birden fazla anten kullanımı ile çeşitlilik sağlanarak, MIMO iletişim teknikleri ile spektral verimlilik ve iletişim kalitesi, erişilmek istenilen yüksekliğe çıkartılabilir. MIMO sistemler bu kazanımı haberleşme linkinin ek gönderim gücünü veya ek gönderim bant genişliğini kullanmadan elde ederler. Bu kazançlar MIMO sisteminde kanal bilgisinin alınmasını ve belirli durumlarda da vericide bilinmesini gerektirir. MIMO sistemler bu kazanımların yanında ekstra anten kullanımından ötürü uzaysal alan artışı ve çok boyutlu sinyal işleme gerekliliğine sebep olarak sisteme sayısal karmaşıklık eklenmesine sebep olabilmektedir.

3.2 OFDM

Yüksek hızlı iletimde, azalan sembol süresinin, kanaldaki gecikmeye göre daha küçük olması semboller arası girişime (Intersymbol Interference, ISI) sebep olmaktadır. Bunun sonucu olarak kanalın frekans seçiciliği artmasıyla sistemin başarım oranı düşecektir. OFDM, kanalın frekans seçiciliğini kaldırarak, kanaldaki semboller arası girişimi engelleyip kanalı düz sönümlemeli bir kanal haline getiren bir tekniktir. Bu sistem, bant genişliliğini birbirine dik alt bantlara bölerek sinyali bu alt kanallardan gönderir. Her bir alt taşıyıcı diğeriyle dikgen olduğundan birbirleriyle girişim yapmamakta ve böylece frekans bandı daha verimli kullanılmaktadır.

OFDM sistemi temel blok diagramı Şekil 4'teki gibidir. Vericide, kullanıcı verileri, seçilen bir modülasyon çeşidi uygulanarak IQ sembol haritası elde edilir. Pilot (referans) semboller eklenerek, sıfır ekleme (zero padding) işlemi uygulanır. Ardından S/P bloğu ile seriden paralele dönüştürme işlemi yapılarak ters hızlı Fourier dönüşümü (IFFT) işlemi gerçekleştirilir. P/S bloğu ile paralel-seri dönüşümü yapıldıktan sonra öntakı (Cyclic Prefix;CP) bloğu ile kanalın etkisine karşı dayanıklı olması için ön ek eklenir. Son olarak, seri dijital veriler dijital-analog dönüştürücü işlemi için D/A bloğundan geçer.

Alıcıda ise gelen analog veri öncelikle dijital veriye dönüştürülür. Ardından ön ek silme işlemi, senkronizasyon kayması engellendikten sonra gerçekleştirilir. S/P bloğu ile seriden paralele dönüştürme işleminin ardından dijital veri FFT işlemine sokulur. FFT bloğunun çıkışına, denkleştirme ve kanal kestirimi uygulanır. Pilot sembollerden yararlanarak kanal kestirimi için en küçük kareler yöntemi kullanılır. Alt-taşıyıcı veriler için kanal kestirimi, pilot sembollerin kanal kestirimi yardımıyla tek boyutlu lineer interpolasyon algoritması yardımıyla yapılır. Bu algoritmalar sayesinde kanal durum bilgileri elde edilir. Dengeleme süreci, kestirilen kanal katsayıları kullanılarak iletilen veriyi elde etmek için uygulanır. Ardından seçilen modülasyon çeşidine göre demodülasyon yapılarak, IQ sembol ayrıştırması gerçekleştirilir.



Şekil 4: OFDM Sistem Blok Diyagramı

3.3 Hüzmeleme

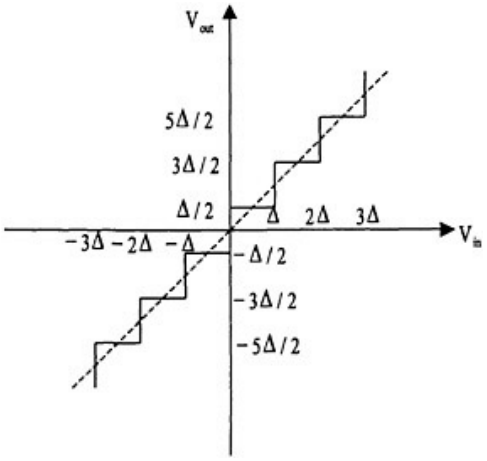
Kablosuz iletişim cihazları arttıkça, kablosuz cihazlar sinyali tüm alana yayarak kablosuz karışım meydana gelmektedir. Hüzmeleme (beamforming), verileri her yönde yaymak yerine, verileri istenilen alıcı yönüne doğru iletir. Direk olarak istenilen cihaza doğru dağıtım yaparak hem kablosuz karışım azaltılarak hem de verinin güvenliği daha kolay sağlanmaktadır. Hüzmeleme teknolojisi (hüzme şekillendirme), sayısal sinyal işleme (Digital Signal Processing, DSP) mantığı ve MIMO sistemine göre şekillenir. Verici sinyalin faz ve göreceli genliğini değiştirerek, yapıcı veya yıkıcı girişim oluşturabilir. Böylece istenilen yöndeki sinyalin diğer yöndeki sinyallere göre daha güçlü olması sağlanır. Hüzmeleme, MIMO sistemin avantajlarına sahiptir. Ayrı antenlerle gönderilen sinyaller birleştirilerek daha güçlü bir sinyal oluşturulabilir. Kanal kalibrasyonu ile fazın değişimine karar verilir. Hüzme şekillendirme için doğru yönü seçmek, kanal kalibrasyonu prosedürüne dayanır. Verici alıcıya boş veri paketi (Null Data Packet, NDP) gönderir ve alıcı paketi aldıktan sonra, geri bildirim matrisini analiz eder ve hesaplar. Verici de bunun üzerine yönlendirme matrisini geri bildirime göre hesaplar. Bu yönlendirme matrisiyle, sinyalin fazı ve genliği düzenlenir ve böylece verici veriyi istenen yöne doğru iletir. Sinyal doğru biçimde yönlendirildiği için enerji en etkili biçimde kullanılmış olur.

Frekans ortamında örnek matris çevirimi (Sample Matrix inversion, SMI) yani post-FFT her bir anten için FFT blok işlemine ihtiyaç duyar ve her bir alt-taşıyıcı için SMI gerçekleştirilir. Anten sayısı ve/veya alt-taşıyıcı sayısı fazla iken, post-FFT SMI karmaşıklığı çok yüksektir. Bu sorunu çözmek için, her alt-taşıyıcı grubu için SMI yerine getirilir. Zaman ortamında SMI (Pre-FFT) ile tüm sistem için sadece bir FFT bloğu ile tüm antenler için çıkış sinyallerine uygulanır. Bu sebeple, Post-FFT SMI gerçeklemesine göre hesaplama yükü çok daha azdır. Tüm alt-taşıyıcılar için aynı hüzmeleme ağırlığında pre-FFT ve post-FFT eşdeğer olsalar da, pre-FFT için gerçek zamanlı BER performansının daha iyi olduğu gözlemlenmiştir [121].

3.4 Kanal Genlik Bilgisinin Nicemlenmesi

Kanal genlikleri düzgün nicemleyici (uniform quantizer) kullanılarak nicemlenebilir. Şekil 5'de gösterilen düzgün nicemleme, Darbe Kod Modülasyonu'nda (PCM) da kullanılan bir yöntem olup, girişte verilen değerleri önceden belirlenmiş olan aralıklara göre seviyelere ayırır ve çıkışında

seviyelere atanan gerilim darbelerini verir. Ancak darbe kod modülasyonunda iletilen işaretlerin alıcıda geri üretilmesi gerektiğinden nicemleme işlemi bir kayıp oluşturmaktadır. Burada işaretin geri üretimi söz konusu olmadığından nicemleme işlemi herhangi bir kayba sebep olmamaktadır. Aksine, sistemde karşılıklı iki nokta için de aynı anahtar çıkarımı sağlamak için gereklidir.



Şekil 5: Nicemleme Giriş-Çıkış Grafiği

Girişe kanal katsayılarının sadece genlik değerleri kullanıldığı için faz kaymasından kaynaklanacak negatif bir etki beklenmemektedir. Nicemleme aralığını aşağıdaki ifadeye göre tanımlayabiliriz;

$$\Delta = \frac{A_{max} - A_{min}}{Q} \tag{1}$$

Burada A işaretin genlik değerini Q ise nicemlenecek düzey sayısını belirtmektedir. Nicemleme düzey sayısı ise kodlama işlemi düşünülerek seçilmesi gerekmektedir. Eğer bir sembolü ifade edecek bit dizisinin uzunluğuna n diyecek olursak nicemleme düzey sayısı aşağıdaki gibi olacaktır;

$$Q = 2^n \tag{2}$$

Sistem modeli de dikkate alındığında nicemleme aralığı Δ'nın anahtar uzunluğunu ve hata oranını belirlemede önemli bir nicelik olduğu gözlemlenebilir. Δ'nın artması ile kod uzunluğu ve anahtarların hata oranını azalmaktadır. Nicemleme aralığının yüksek olması anahtarların uyuşmasını arttırsa da anahtarın güvenilirliğini azaltacaktır.

Nicemleme işleminden sonra oluşturulan genlik seviyeleri belirlenen kod dizisine göre bitlere çevrilerek anahtar üretimi tamamlanacaktır. Alıcı ve vericilerde seçilen nicemleme aralığı ve kod sözcüklerinin aynı olması anahtar üretimi için kritik önem taşımaktadır.

3.5 Kanal Yön Bilgisinin Nicemlenmesi

Kullanıcıya ait kanal durum bilgisi (CSI), limitli geri besleme kanalından alıcıda nicemlenerek vericiye iletilir. Kullanıcının kanal vektörü $\mathbf{h} \in \mathcal{C}^{N_t \times 1}$ her elemanı ortalaması 0 ve varyansı 1 olan karmaşık Gauss dağılımı ile modellenir. Burada N_t vericideki anten sayısıdır. Kanal yön bilgisi (CDI)

$$\mathbf{g} = \frac{\mathbf{h}}{\|\mathbf{h}\|} \tag{3}$$

ve kanal kalite bilgisini (CQI) $\|\mathbf{h}\|$ şeklinde ifade edilir.

Kullanıcı ait kanal yön bilgisi vektörü olan $\mathbf{g}$ daha önceden belirlenmiş 2^B boyutundaki kod kitapçığından seçilmiş $\mathbf{c}$'ye nicemlemektedir. B burada nicemleme için kullanılan bit sayısını ifade etmektedir. Kod kitapçığı $\mathcal{C} = \{\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_i, \ldots, \mathbf{c}_{2^B}\}$ olup rasgele vektör nicemlemeye (RVQ), Lloyd gibi farklı algoritmalarına dayalı olarak tasarlanabilir. Burada B nicemleme için kullanılan bir sayısını ifade eder.

CDI için en iyi kod indeksi aşağıdaki gibi bulunur:

$$i^* = \arg \max_{1 \le i \le 2^B} \left| \mathbf{g}^H \mathbf{c}_i \right| \tag{4}$$

Takiben hüzmeleme vektörü aşağıdaki gibi elde edilir:

$$\mathbf{w} = \mathbf{c}_{i^*} \tag{5}$$

RVQ dayalı kod kitapçığı için $\mathbf{g}$ ile $\mathbf{c}_{i^*}$ arasındaki ilişki aşağıdaki gibi tanımlanır:

$$\mathbf{g} = \mathbf{c}_{i^*} \cos\theta + \mathbf{g}^{\perp} \sin\theta, \tag{6}$$

Burada $\mathbf{g}^{\perp}$, $\mathbf{c}_{i^*}$'ya dik olan bir birim norm vektörünü ifade ederken, nicemleme hatası açısı $\theta = \angle(\mathbf{g}, \mathbf{c}_{i^*})$ olup $\mathbb{E}\{\sin\theta\} \le 2^{-B/(N_t-1)}$'dir.

3.6 Döndürülmüş Kod Kitapçığı

CDI için normalize edilmiş bağımsız ve aynı dağılımlı (i.i.d.) kod kitapçıkları yerine yerel bölgeler (local region) için küresel bölgeye uygun döndürülmüş kitapçığı tasarımı yapılabilir. Bunun için N_t, 2^B, merkezi $\mathbf{o}$, küresel bölge açısı için eşik değeri ϵ parametreleri olan yerel Grassmannian çizgi paketi (Grassmannian line packing) kullanılır. En büyük minimum kirişsel uzaklığına (largest minimum chordal distance) dayalı yönteme göre $\mathcal{B}_\epsilon(\mathbf{o})$ küresel bölgesi için nicemleme yapılır ve kod kitapçığı $\mathcal{C}^\epsilon = [\mathbf{c}_1^\epsilon, \mathbf{c}_2^\epsilon, \ldots, \mathbf{c}_{2^B}^\epsilon]$ oluşturulur.

Daha sonra $\boldsymbol{\phi} \in \mathcal{C}^{N_t \times 1}$ açısına göre herbir kod kelimesi döndürme matrisi uygulanarak döndürülür.

$$\mathbf{c}_j^{rot} = \mathbf{U}^{rot} \mathbf{c}_j^\epsilon; j = 1, ..., 2^B \tag{7}$$

Burada döndürme matrisi $\mathbf{U}^{rot} = \boldsymbol{\phi}\mathbf{o}^{-1}$ olarak tanımlanır.

3.7 Diferansiyel Kod Kitapçığı

Durağan olmayan kanallar için kanalın zamanda ilintisinin modellenmesi için ile kullanıcının kanalının zamanda değişimi Gauss-Markov süreci olarak tanımlanır:

$$\mathbf{h}_\tau = z\mathbf{h}_{\tau-1} + \sqrt{1-z^2}a_\tau \tag{8}$$

Burada a_τ karmaşık normal Gauss dağılımına sahip inovasyon sürecini belirtmektedir. z ise kanalın zamansal ilinti katsayısı olup $(0 \leq z \leq 1)$ kanalın ardışık zaman aralıklarında birbiriyle ilişkisinin ölçütüdür. Eğer z büyük bir değere sahipse, bu durum $\mathbf{h}_{\tau-1}$ vektörü ile $\mathbf{h}_\tau$ vektörünün ilintisinin yüksek olduğu anlamına gelir. Beklendiği üzere, yüksek z değerleri için diferansiyel kod kitapçığının performansı daha iyi olmaktadır.

Diferansiyel kod kitapçığının algoritması aşağıdaki gibi gerçekleştirilmiştir:

- $\tau = 0$ anında:
  İlk zaman dilimindeki kanal bilgisi rasgele vektör nicemleyici kullanılarak oluşturulan başlangıç kod kitapçığı kullanılarak, minimum uzaklığa göre nicemlenir.

$$j^* = \arg \min_{1 \leq j \leq 2^B} |1 - \mathbf{g}_0{}^H \mathbf{c}_j| \tag{9}$$

  Daha sonra hüzmeleme vektörü aşağıdaki gibi elde edilir:

$$\mathbf{w}_0 = \mathbf{c}_{j^*} \tag{10}$$

- $\tau = 1, 2, ...\tau_{max}$ anları için:
  Önceden belirlenmiş temel kutupsal kap (polar-cap) diferansiyel kod kitapçığı kullanılır. Temel kutupsal kap diferansiyel kod kitapçığı $\tilde{\mathcal{W}}^\tau$'nin oluşturulması için,

$$\tilde{\mathcal{W}}^\tau = \left\{ \tilde{\mathbf{w}}_{1,\tau}, \begin{bmatrix} \sqrt{1-\delta_\tau^2} \\ \delta_\tau \mathbf{f_2} \end{bmatrix}, \ldots, \begin{bmatrix} \sqrt{1-\delta_\tau^2} \\ \delta_\tau \mathbf{f_{2^B}} \end{bmatrix} \right\} \tag{11}$$

  yapısı kullanılmıştır.

  $\tilde{\mathbf{w}}_{1,\tau}$ herhangi bir birim vektör olabilir. Bu çalışmada $\tilde{\mathbf{w}}_{1,\tau} = [1, 0, \ldots, 0]^T$ olarak seçilmiştir. Kutupsal kap boyutunu belirten δ_τ, sistem preformansını önemli ölçüde etkilemektedir. Bu parametre uyarlamalı ya da sabit olarak ayarlanabilir. $\tilde{\mathbf{w}}_{1,\tau}$ ve δ_τ'nun seçilmesiyle kutupsal kabın çevresine yerleştirilmiş kod sözcükleri oluşturulabilir. Diğer kod sözcükleri karmaşık Grasmannian çizgi paketlemesi vektörleri (complex Grassmannian Line Packing), $\{\mathbf{f_2}, \mathbf{f_3}, \ldots, \mathbf{f}_{2^B}\}$ ile oluşturulmuştur. Burada $\mathbf{f}_i \in \mathcal{C}^{(N_t-1)\times 1}$'dır. Bunun sebebi Grasmannian çizgi paketlemesi kod kitapçığının bağımsız ve aynı dağımlı Rayleigh sönümlemeli kanallar için bilinen en iyi yöntem olmasıdır.

  Kutupsal kap kod kitapçığı bir kere oluşturulduktan sonra farklı τ anları için tekrar tekrar kullanılabilir. Kod kitapçığının belirlenmesinden sonra, kullanıcı ve verici $\tilde{\mathbf{w}}_{1,\tau}$ vektörünü $\hat{\mathbf{h}}_{\tau-1}$ yönüne çevirecek olan rotasyon matrisi $\mathbf{R}_{\hat{h}_{\tau-1}}$'i oluşturur.

Rotasyon fonksiyonu aşağıdaki gibi tanımlanır:

$$\mathbf{r} : \mathcal{B}_{\delta_\tau}(\tilde{\mathbf{w}}_{1,\tau}) \mapsto \mathcal{B}_{\delta_\tau}(\hat{\mathbf{h}}_{\tau-1}) \tag{12}$$

$$\hat{\mathbf{h}}_{\tau-1} = \mathbf{r}(\hat{\mathbf{h}}_{\tau-1})\tilde{\mathbf{w}}_{1,\tau} \tag{13}$$

$$= \mathbf{R}_{\hat{h}_{\tau-1}}\tilde{\mathbf{w}}_{1,\tau} \tag{14}$$

Rotasyon matrisinin oluşturulabilmesi için Householder transformasyonu kullanılmıştır:

$$\mathbf{v} = \tilde{\mathbf{w}}_{1,\tau} - \hat{\mathbf{h}}_{\tau-1} \tag{15}$$

$$\mathbf{R}_{\hat{h}_{\tau-1}} = \mathbf{I} - \frac{\mathbf{v}\mathbf{v}^\dagger}{\mathbf{v}^\dagger\tilde{\mathbf{w}}_{1,\tau}} \tag{16}$$

Rotasyon matrisinin Householder transformasyonuyla yukarıdaki gibi elde edilmesinden sonra, rotasyon matrisi ile bütün temel kutupsal kap kitapçığı döndürülür.

$$\mathcal{W}^\tau = \left\{\mathbf{R}_{\hat{h}_{\tau-1}}\tilde{\mathbf{w}}_{j,\tau}; \quad j = 1, 2, ..., 2^B\right\} \tag{17}$$

Temel kutupsal kod kitapçığının her bir kolonu rotasyon matrisi ile çarpılarak döndürülmüş olan yeni kod kitapçığı $\mathcal{W}^\tau = \left\{\mathbf{w}_{1,\tau}, \mathbf{w}_{2,\tau}, \ldots, \mathbf{w}_{2^B,\tau}\right\}$ oluşturulmuştur. Kullanıcı τ anındaki kanal bilgisini bu kod kitapçığına göre nicemler ve vericiye yollar. Verici ise bu bilgiyi hüzmeleyici vektörü $\mathbf{w}_\tau$ olarak kullanır.

$$j^* = \arg\min_{1<k<2^B} |1 - \mathbf{g}_\tau{}^H\mathbf{w}_{j,\tau}| \tag{18}$$

$$\mathbf{w}_\tau = \mathbf{w}_{j^*,\tau} \tag{19}$$

- $\tau = \tau_{max} + 1$

  Belirlenen τ_{max} süresinden sonraki zamanlarda işlemler sıfırlanır. τ_{max} süresi kanalın tutarlı olduğu süre (coherence time) olarak seçilebilir.

3.8 Eşik Değerine Dayalı Kullanıcı Seçimi

K aktif kullanıcıya sahip olan sistemlerde $K > N_t$ iken çoklu kullanıcı çeşitliliğine açığa çıkararak güvenlik kapasitesini enbüyüklemek için kanal kazancı açısından en iyi kullanıcı seçilebilir. Zayıf kanallı yetkili kullanıcılar (düşük norm), vericide yapılan bu seçimde rol almamalıdır. Bu sebeple kullanıcı tarafında eşik değerine dayalı seçimi sağlayan $\mathcal{T}_1$ kriteri ile bu kullanıcıların kanal durum bilgilerini vericiye iletmeleri önlenir ve böylece geri besleme yükü azaltılır [122].

$\mathcal{T}_1$ kriteri, belirlenen eşik değerini sağlayan kullanıcıları seçerek bir $\mathcal{U}_1$ kümesini kurmaktadır.

$$\mathcal{U}_1 = \left\{k \in K : \|\mathbf{h}_k\|^2 > \gamma_{th}\right\}. \tag{20}$$

Burada γ_{th} kanal normu için kullanılan eşik değeridir.

Bu eşik değerinin belirlenmesi, ortalama olarak $\bar{K}$ kadar yetkili kullanıcının kanal durum bilgisini vericiye göndermesininin sağlanması amacıyla analitik olarak elde edilebilir.

$$\bar{K} = KPr\left\{k \in \mathcal{U}_1\right\} = KPr\left\{\|\mathbf{h}_k\|^2 > \gamma_{th}\right\}. \tag{21}$$

$\mathcal{U}_1$ kümesi tamamlanmamış gamma dağılımı ile belirlenmekte olup aşağıdaki sınır değeri verilebilir:

$$\left[1-\exp(-\beta\gamma_{th}))\right]^{N_t} \leq \int_0^{\gamma_{th}} f_\gamma(\gamma)d\gamma \leq \left[1-\exp(-\gamma_{th}))\right]^{N_t}, \tag{22}$$

Bu denklemde $\beta = (N_t!)^{\frac{-1}{N_t}}$ olup, olasılık yoğunluk fonksiyonu $f_\gamma(\gamma)$ ise χ_2^2'dir.

Böylece,

$$Pr\left\{k \in \mathcal{U}_1\right\} = \sum_{b=0}^{N_t-1} \frac{\exp(-\gamma_{th})(\gamma_{th})^b}{b!} \tag{23}$$

ifadesi elde edilebilir.

Böylece kanal durum bilgilerini vericiye geri besleme linki üzerinden gönderen ortalama kullanıcı sayısı analitik olarak aşağıda gösterildiği gibi hesaplanabilir:

$$\bar{K} = K\sum_{b=0}^{N_t-1} \frac{\exp(-\gamma_{th})(\gamma_{th})^b}{b!} \tag{24}$$

Daha sonra vericide kanal durum bilgisi limitli geri besleme kanalından iletilen tüm yetkili kullanıcılar arasında en iyi kanal kazancına sahip kullanıcı seçilir:

$$k = \arg\max_{j\in\mathcal{U}_1} \|\mathbf{h}_j\|^2 \tag{25}$$

3.9 Yarı-dik Kriterine Dayalı Kullanıcı Seçimi

K aktif kullanıcıya sahip olan sistemlerde $K > N_t$ iken çoklu kullanıcı çeşitliliğine açığa çıkararıp çoklu kullanıcıya aynı anda hizmet vererek güvenlik kapasitesini enbüyüklemek için, en iyi $M \leq N_t$ kullanıcı kombinasyonunu seçmek önemlidir. Bu yüzden, uygun olmayan koşullara sahip kullanıcılar alıcı tarafında elenmeli ve kanal durum bilgilerini vericiye iletmemelidirler.

Yarı-dik kullanıcı seçim kriteri, kanal yön vektörleri birbirine en dik olan kullanıcıları seçmektedir. Her kullanıcı, aynı N_t rasgele birim dik vektörleri $\boldsymbol{\phi}_i \in \mathcal{C}^{N_t\times 1}$, $i = 1,\ldots,N_t$'yi oluşturmaktadır. Ardından, kullanıcılar $\boldsymbol{\phi}_i$ ile kendi kanal yönleri arasındaki dikliği aşağıdaki gibi ölçülür:

$$d^2(\mathbf{g}_k, \boldsymbol{\phi}_i) = 1 - |\mathbf{g}_k^H \boldsymbol{\phi}_i|^2 \tag{26}$$

Denklem (26)'deki ölçüm metriğini kullanarak, her yarı-diklik için eşik değeri $0 < \epsilon < 1$ değeri için $\mathbf{o}$ merkezli ve ϵ yarıçaplı bir küresel kap $\mathcal{O}^{N_t}$ üzerinde açık küme olarak tanımlanabilir.

$$\mathcal{B}_\epsilon(\mathbf{o}) = \left\{\mathbf{g}_k \in \mathcal{O}^{N_t} : d^2(\mathbf{g}_k, \mathbf{o}) \leq \epsilon_{th}\right\} \tag{27}$$

Ardından, yarı-dik seçim kriteri olan $\mathcal{T}_3$ algoritması [122] uygulanır:

$$\mathcal{T}_3 = \left\{ k \in K : \mathbf{g}_k \in \bigcup_{i=1}^{N_t} \mathcal{B}_\epsilon(\boldsymbol{\phi}_i) \text{ and } \|\mathbf{h}_k\|^2 \geq \gamma_{th} \right\} \tag{28}$$

Bu eşik değerleri ile, yarı-diklik koşulunu sağlayan ama düşük norma sahip olan kullanıcılar elenmiştir. Bunun nedeni ise seçilmiş kullanıcının kanal kaliteisinin güvenlik kapasitesi toplamını doğrudan etkilemesidir.

Sonuç olarak, ortalama $\bar{K}$ kullanıcının kanal durum bilgilerini vericiye yollamasına izin verilmiştir ve verici bunlardan en yüksek norma sahip M tanesini güvenli haberleşme için seçmektedir.

Eşik değerlerine, ortalama $\bar{K}$ kullanıcıya izin vermek için

$$\bar{K} = KN_t \sum_{b=0}^{N_t-1} \frac{\exp(-\gamma_{th})(\gamma_{th})^b}{b!} \epsilon^{N_t-1} \tag{29}$$

ile karar verilir.

$\mathcal{T}_3$ kriteri ile seçilmiş kullanıcıların nicemleme hatasını düşürmek için döndürülmiş kod kitapçığı kullanılabilir.

3.10 Yazılım Tabanlı Radyo Teknolojisi

Kablosuz haberleşme teknolojileri günümüzde mobil iletişim aygıtlarından uydu haberleşmesine kadar pek çok farklı alanda kullanılmaktadır. Kablosuz haberleşmede bilgi aktarımı radyo dalgaları ile gerçekleşmektedir. Kablosuz haberleşme sistemlerinin yaygınlaşması ile spektrum yönetimi en can alıcı nokta haline gelmiştir. Kablolu iletişimden kablosuz iletişime geçişle birlikte, kablosuz cihazların kullanım alanı yaygınlaştıkça artan taleple radyo frekans spektrumu için kısıtlı olan frekans bantlarının kullanımı daha da değerli hale gelmiştir. Bu da, radyo frekans spektrumunun statik olarak paylaşılmasındansa dinamik olarak paylaştırılmasının daha verimli hale gelmesine sebep olmuştur ve haberleşme sektörü için yazılım tabanlı radyolar odak noktası haline gelmiştir.

Yazılım tabanlı radyolar (SDR), modülasyon, demodülasyon, kodlama, filtreleme, frekans seçimi, haberleşme protokolleri gibi işlemlerin kapsamlı bir donanım üzerinde yazılımla gerçeklendiği bir radyo haberleşme sistemidir. Yazılım tabanlı radyoya yönelik ilk fikirler 1990'lı yıllarda ortaya atılmıştır. Sayısal İşaret işleme işlemleri için sayısal işaret işlemcisi (Digital Signal Processing, DSP), Alanda Programlanabilir Kapı Dizileri (Field Programmable Gate Array, FPGA) ve genel amaçlı işlemciler kullanmaktadır.

Radyo sistemlerindeki donanım üzerine dinamik şekilde sinyal işleme teknikleri ayarlanıp programlama işlemi yapılarak, değişiklikler kolayca sağlanmaktadır. 2000'li yıllara gelindiğinde ise, FPGA, DSP ve ADC gibi elektronik ekipmanların performansları önemli ölçüde artarken maliyetleri düşmüştür. Haberleşme teknolojilerinin gelişmesi ve akıllı telefonların kullanımının yaygınlaşması ile yazılım tabanlı radyo uygulamaları oldukça yaygın bir kullanım oranına ulaşmıştır.

Yazılım tabanlı radyolarla radyo sinyallerinin alınması ve gönderilmesi işlemlerinin donanım

üzerinde çalışan yazılımla gerçeklenebilmektedir. Herhangi bir frekans bandında çalışarak, o bandda modülasyonlu sinyal gönderimi, alınan sinyalin demodülasyon işlemi gibi işlevleri mümkün olan en az donanım ile dinamik bir biçimde gerçekleyebilme yeteneğine sahiptir. Yazılım tabanlı radyolar çok modlu, çok bandlı ve çok fonksiyonlu bu yapısıyla ucuz ve etkili çözümler getirir. Yazılım tabanlı radyoların en önemli özellikleri arasında esneklik, sürekli bağlantı, yeniden şekillendirilebilme ve birlikte çalışılabilirlik vardır. Yazılım tabanlı radyo teknolojisi, haberleşme sistemleri için artık akıllı ve öğrenilebilirlik açısından gelişim imkanı vermektedir.

Askeri amaçlı başlayan yazılım tabanlı radyolar, sivil amaçlar için kullanılabilen farklı standartlarla çalışan ikinci üçüncü nesil haberleşme sistemleri ve telsiz haberleşme sistemlerinde geniş uygulama alanları bulmaktadır. Frekans spektrumunun dinamik olarak kullanılabilmesi, donanım aracılığıyla yapılabilecek değişikliklerin yazılımla daha rahat bir biçimde yapabilmesi maliyetleri düşürmesi büyük bir avantajdır. Sistemin yazılım ile güncelleştirilebilmesi ve farklı haberleşme standartlarının hızlı ve uyumlu bir biçimde geçişi büyük kolaylıklar sağlamaktadır.

3.10.1 USRP

USRP (Universal Software Radio Peripheral) cihazları projede kullanılan yazılım tabanlı radyolardır. Genel amaçlı bir anakart olan USRP birimleri üzerinde 4 tane yüksek hızlı analogtan sayısala (analog to digital converter, ADC) çeviricileri, 4 tane sayısaldan analoga (digital to analog converter, DAC) çeviricileri, bir tane alanda programlanabilir kapı dizileri (Field Programmable Gate Array, FPGA) ve birkaç giriş ve çıkışa sahiptir. USRP birimleri, yazılım tabanlı radyo çalışmaları için çok uygun olup, esnek, dinamik, açık kaynaklı ve yüksek hızlı donanımlardır. GNU (GNU's Not Unix) radyo yazılımı doğrudan cihaz ile kolay bir şekilde iletişim kurabilmektedir.

Açık kaynak yazılım tabanlı radyo geliştirme platformu olan GNU Radyo yazılımı USRP birimlerinin gelişiminde büyük katkılar sağlamaktadır. USRP birimleri radyo frekans ortamı ile bilgisayar arasında bağlantıyı sağlamaktadır. Cihaz bilgisayar arayüzüne radyo sinyallerini ulaştırarak, geri kalan işlemleri arayüzdeki sinyal işleme yazılımı ile sağlar. Yani esas görevi ADC, interpolasyon gibi yüksek hızda genel amaçlı işlemleri FPGA devresi üzerinde yaparak, dalga fonksiyonları ile ilgili işlemler bilgisayar yazılımı üzerinde tamamlamaktır. Yazılım tabanlı radyoların yapısı hakkında Şekil 6 fikir vermektedir.

3.10.2 Kullanılan Donanım ve Yazılım Bilgisi

Projede yazılım tabanlı radyo olarak NI (National Instruments) USRP 2921 modeli ve bu cihaz için özel kütüphanelere sahip LabVIEW yazılımı kullanılmıştır.

NI USRP 2921 NI USRP 2921, proje içinde kullanılan, USRP cihazlarının bir modelidir. Hem alıcı hem verici işlevinde kullanılabilen USRP birimi 2.4-2.5 GHz ile 4.9-5.9 GHz frekans aralıklarında çalışabilmektedir. NI USRP 2921, yarı duplex özelliğe sahip bir cihazdır ve aynı anda sinyal iletimi ve alımı yapamaz. Verici işlevi için, maksimum çıkış gücü 17dBm ile 20

dBm arasında değişiklik gösterirken, maksimum giriş gücü ise -15 dBm olarak ifade edilmektedir. 20 MHz aralığında, 16 bitlik örnekleme ile maksimum desteklediği I/Q örnekleme hızı 25 MS/s'dir. LabVIEW Haberleşme Sistem Dizayn Yazılımı ile birlikte çalışarak, tek kanallı sistemlerden, MIMO kablosuz haberleşme sistem dizaynına kadar geniş yelpazede bir kullanım sağlamaktadır.

LabVIEW LabVIEW, Laboratory Virtual Instrument Engineering Workbench kelimelerinin kısaltılmasından elde edilen bir isimdir ve bir programlama ortamını tanımlar. LabVIEW geleneksel programlama dillerinden farklıdır ve klasik programlama dillerinden daha fazlasını içermektedir. LabVIEW, bilim insanları ve mühendisler gibi kişiler için tasarlanmış, interaktif bir yazılım geliştirme ve uygulama sistemidir. Grafiksel bir programlama dili olan LabVIEW, küçük grafiksel ikonlar ve kablolar ile akış diyagramları oluşturmaya ve oluşturulan programları nesne tabanlı kullanarak, küçük birçok program parçalarını birleştirmeye yaramaktadır. Metin tabanlı dillere göre kullanımı daha kolay olan LabVIEW, daha görsel bir platform sunmaktadır. Endüstride büyük kullanım alanı mevcuttur ve mühendislik, istatistik, kimya, fizik gibi birçok alanda kolaylıklar sağlamaktadır.

National Instrument bünyesinde geliştirilen LabVIEW veri toplama kartları, modüler enstrümantasyon sistemleri, kompakt kartlar ile test ölçme ve kontrol sistemleri için önemli yer tutmaktadır. LabVIEW'de; sinyal işleme, ölçüm, veri haberleşmesi gibi fonksiyon kütüphaneleri mevcuttur. Bu fonksiyon kategorilerinin içinde bir haberleşme sistemi oluşturulabilecek haberleşme işlemleri için gerekli kütüphaneler vardır.

LabVIEW ile programlama mantığı, geleneksel programlamayla yazılan kod mantığına benzemekle birlikte, veri yolu bağlantıları kontrol adı verilen nesne blokları ile program akışı sağlanır. Veriler elektrik kablosuna benzer çizgi üzerinden bağlı olduğu kontrole geçer. LabVIEW'de iki pencere vardır; Görsel nesnelerin bulunduğu ön panel (Front Panel) ve program akışının bulunduğu blok diyagram (Block Diagram) penceresidir.

Bu pencerede, fonksiyonlar (functions) tablosundan istenilen nesneler yerleştirilerek, sanal kablolarla bağlanarak program uygulumaya geçilebilir. Bu nesneler, sanal cihaz (VI-virtual instrument) olarak adlandırılır. LabVIEW'de üç adet VI tipi vardır. Bunlar kontrol (control), gösterge (indicator) ve sabit (constant) nesne tipleridir. Kontrol VI'ları ile, kullanıcı veri girişi yapar, parametre değerleri verilerek programın sonucu gösterge VI'ı ile kullanıcıya sunulur. Sabit VI ise, sabit değerlere sahip girdilerdir.

Senkronizasyon SDR tabanlı MIMO sistem uygulanırken, en sık karşılaşılan zorluklardan biri, biri verici ve diğeri alıcı için kullanılan ikişer adet USRP birimlerinin senkronizasyon işlemidir. Güçlü sistem performansı sağlamak için, her bir düğümün birbiriyle koordine olarak çalışması gerekmektedir. Özellikle eğer OFDM tekniği MIMO ayarıyla oluşturulduysa, OFDM'in işlevselliğinden faydalanmak adına, noktalar arasındaki senkronizasyonun önemi daha da artmaktadır. Hem donanım hem yazılım ayarlarını içeren düzenlemelerle birkaç adımda senkronizasyon problemi çözülebilmektedir.

Senkronizasyon kaynağı olarak testlerde NI PXI-6683 modülü kullanılmıştır. Bu modül, ana

saate bağlı GPS modülünden 10 MHz lik senkronizasyon saat kaynağını sağlamaktadır. İki harici 10 MHz ve bir PPS sinyali, kablo üzerinden bir verici ve alıcı USRP birimine iletilir. İkinci verici ve alıcı USRP birimleri ise bu kablolara bağlı değillerdir, her biri, senkron edilen birinci alıcı ve verici USRP birimine MIMO kabloları üzerinden eş olarak kullanılarak senkronize edilir. Ek olarak, senkronizasyon sinyallerini daha iyi iletmek için, yazılım ve donanım bileşenleri arasındaki senkronizasyon ilintinin doğruluğu için, LabVIEW kodunda da düzenlemeler yapıldı. Böylelikle, yazılım ve donanım bileşenlerinin bağlantı senkronizasyonu testlerde bu şekilde sağlanmıştır.

3.11 Karşılıklı Kanal Özelliği

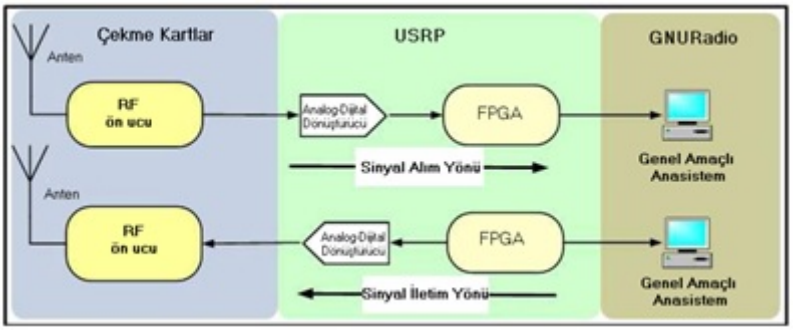
Karşılıklı kanal özelliği, elektromanyetik dalganın tersinir olmasından dolayı ortaya çıkan bir gerçektir. Elektromanyetik dalga, her iki yönde de yansıma, kırınım, dağılım gibi aynı fiziksel bozulmalara maruz kalır. Eğer bir elektromanyetik dalga, belirli bir yol üzerinden A noktasından B noktasına ulaşıyorsa, B noktasından A noktasına da elektromanyetik dalga aynı yol üzerinden yayılır. Bu aynı ulaşım yolu, iki durum için de aynı yol zayıflatmasını, gecikmesini ve faz kaymasını beraberinde getirecektir. Bir kablosuz haberleşme sisteminde ise, bu durum A'dan B'ye giden kanal ile B'den A'ya giden kanalın aynı olmasını ifade edecektir. Bu nedenle, aynı frekans bandının kullanıldığı hücresel bir haberleşme sisteminde yukarı yönlü bağlantı kanalı ile aşağı yönlü bağlantı kanalı teorik olarak aynıdır. Üst katmanlarda oluşturulan güvenlik sistemlerinden ziyade, fiziksel katmandaki güvenlik sistemlerinde, kanalın özellikleri çok önemli yer tutar. Kanalın karşılıklı olma özelliğinin yardımıyla güvenlik anahtarı üretimi, fiziksel katman güvenlik yönteminin can alıcı noktasıdır.

Elektromanyetik dalganın karşılıklı olma teoremine göre karşılıklı kanal modeli [139]'da şu şekilde ifade edilir: A ve B düğümleri, sırasıyla anten sayıları M ve N olarak düşünülmektedir. Sistem, temelband işlemi sırasında üç doğrudal filtrenin ardışık olarak dizilmesi ve toplamsal beyaz Gauss gürültüsü ile modellenmiştir. Bu model Şekil 8'te gösterilmektedir.

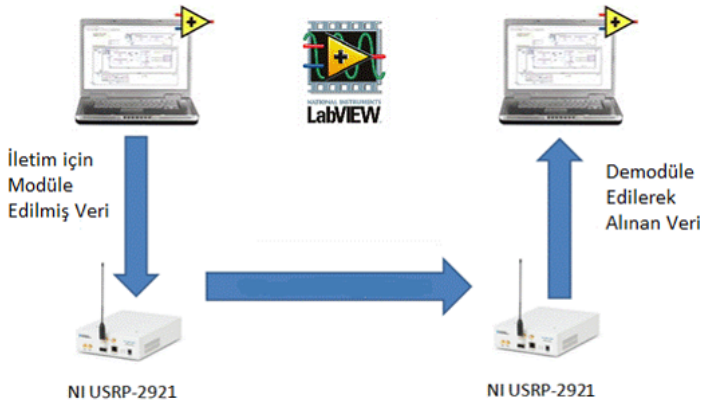
Diagramın üst kısmı, A'dan B'ye iletişimi temsil ederken, alt kısım ise B'den A'ya olan iletişimi temsil etmektedir. T_A, $M \times M$ boyutlu bir matris şeklinde A düğümünün verici devresindeki filtreleme operasyonuna, H(t) ise elekromanyetik kanalın dürtü yanıtlarını içeren (her bir verici-alıcı anten çifti için) $N \times M$ boyutlu bir matrise karşılık gelmektedir. R_B ise B düğümünün alıcı devresindeki filtreleme operasyonunun $N \times N$ boyutlu bir matris şeklindeki ifadesidir. Simetrik bir biçimde, T_B ve R_A sırasıyla B düğümünün verici devresindeki, A düğümünün alıcı devresindeki filtreleme operasyonunu göstermektedir.

Basitlik açısından n_A, n_B gürültüleri, üç filtrenin kaskadının arkasından eklenmiştir, yani alıcı devre ile elektromanyetik kanal arasında görülmektedir.

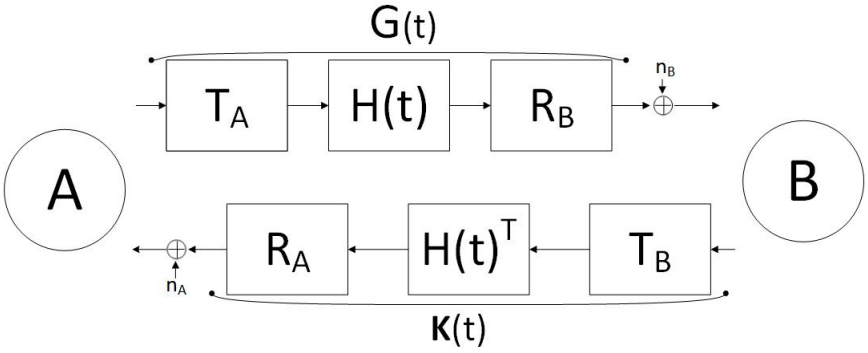
Devre karakteristikleri zamana (t) bağlı değildir, çünkü bu karakteristiklerin değişimi, kanalın varyasyonundan çok daha yavaştır. Her iki yönde iletimin, kanalın uyum (evreuyum) zamanından daha kısa süreli bir zaman diliminde meydana geldiği varsayıldığında, elektromanyetik kanalın karşılıklı olma teoremi, iki yönde de her anten çifti için dürtü yanıtının aynı olduğunu garantiler, bu yüzden $H(t, \tau)$ filtresi iki yönde de aynıdır (anten dizisine bağlı olarak transpozesi alınması gerekebilir).



Şekil 6: Yazılım Tabanlı Radyoların USRP ile Gerçeklenmesinin Blok Diyagramı



Şekil 7: Sistemin Genel İşleyişi



Şekil 8: Karşılıklı Kanal Modeli

Burada * konvolüsyon işlemini, τ gecikmeyi belirtmek üzere; A düğümünden B düğümüne olan gürültüsüz kanal için birleşik dürtü yanıtı aşağıdaki formülasyonda görülmektedir.

$$G(t,\tau) = R_B(\tau) * H(t,\tau) * T_A(\tau) \tag{30}$$

$G(t,\tau)$ için de kanal vektörü h_{AB} ile gösterilir. B düğümünden A düğümüne gürültüsüz kanalın birleşik dürtü yanıtı ise,

$$K(t,\tau) = R_A(\tau) * H(t,\tau)^T * T_B(\tau) \tag{31}$$

şeklindedir. Aynı şekilde kanal vektörü, $K(t,\tau)$ için h_{BA} şeklinde ifade edilebilir. Birleşik dürtü yanıtları zamanla değişmez olduğu düşünüldüğünde kanal vektörlerine ulaşılabilir. B düğümü için $G(t,\tau)$ bilgisi klasik kanal kestirimi ile kolayca elde edilebilir, aynı şekilde A düğümü de $K(t,\tau)$ dürtü yanıtını tahmin edebilir.

Hücresel sistemde, baz istasyonundan kullanıcıya giden bağlantıya aşağı yönlü bağlantı, kullanıcıdan baz istasyonuna giden bağlantıya yukarı yönlü bağlantı denir. Yukarı yönlü bağlantı için kanal durum bilgisi elde etmek için, kullanıcılar baz istasyonuna kılavuz (pilot) sembolleri iletirler, daha sonra baz istasyonu bu kılavuz sembolleri kullanarak yukarı yönlü bağlantı kanalını tahmin eder. Tahmin edilen yukarı yönlü bağlantı kanalı, yani A noktasında B noktasına olan kanal h_{AB} olmak üzere, $M \times N$ boyutunda bir matristir. Karşılıklı kanal durumu sayesinde, aşağı yönlü bağlantı kanalının yukarı yönlü bağlantı kanal matrisinden direkt olarak, $h_{BA} = (h_{AB})^T$ şeklinde elde edilebileceği öngörülmüştür [140].

4 Bulgular

4.1 Durağan kanallar için güvenli MISO sistemi

Bu bölümde durağan kanal yapısına sahip güvenli MISO sistemlerinde çoklu kullanıcı çeşitlemesini ortaya çıkaracak şekilde en iyi tek yetkili kullanıcının seçilmesi ile güvenli haberleşme yapılması sağlanmıştır. Bunun için tüm yetkili kullanıcılara ait kanalları elde etmek gerekmektedir. Kanal durum bilgisinin verici tarafında bilinmesi için, yetkili kullanıcılar baz istasyonuna kanal durum bilgilerini nicemleyerek iletirler. Verici tarafında haberleşme için seçilme olasılığı düşük olan yetkili kullanıcıların kanal bilgilerini iletilmesi, yetkili kullanıcı tarafında yapılan eşik değerine dayalı kullanıcı seçimi ile önlenebilir. Sistem geri besleme yükü (overhead) eşik değerine dayalı yetkili kullanıcı seçim algoritması ile tüm kullanıcıların kanal durum bilgilerini vericiye göndermesi engellenerek önemli ölçüde azaltılmaktadır. Eşik değerine dayalı kullanıcı seçim algoritmasının güvenli haberleşme sisteminin performansı üzerine etkisi, tek bir gizli dinleyici olduğu ve vericide gizli dinleyicinin kanal bilgisinin bilinmediği durumu ile birden fazla gizli dinleyici olduğu ve gizli dinleyicinin kanal durum bilgisinin vericide bilinmediği ve bilindiği durum için sunulmuştur.

Sistem modeli olarak K aktif yetkili kullanıcı arasından seçilen tek yetkili kullanıcının güvenli haberleşme yaptığı MISO sistemi gözönünde bulundurulmuştur. N_t verici antene sahip baz istasyonu (Alice) gizli mesajları seçilmiş tek antene sahip yetkili kullanıcıya (Bob) iletmeyi amaçlamaktadır. Güvenlik kapasitesini en büyüklemek için kanal kazancı açısından en iyi olan yetkili kullanıcı Alice'de seçilir. Sistemde birbirleriyle işbirliği yapan N_e tek antenli gizli dinleyici (Eve) bulunmaktadır. İşbirlikçi gizli dinleyiler N_e antene sahip tek bir gizli dinleyici olarak da görülebilir. Öncelikle gizli dinleyicinin kanal durum bilgisinin vericide olmadığı varsayılmıştır. Bu durumda, verici gizli dinleyicinin algısını bozmak için dış uzaya yapay gürültü üretilir. Gizli dinleyicinin kanal durum bilgilerinin vericide bilinmediği durum pratikde karşılaşılması kuvvetle muhtemel senaryoya uygun olarak oluşturulmuştur. Yetkili kullanıcının kanal durum bilgisinin vericide tam ve nicemlenmiş (quantized) olarak bilindiği iki farklı durum için irdelenmiştir.

Seçilen k kullanıcısı için yapay gürültü eklenerek iletilen sinyal vektörü $\mathbf{x}_k$:

$$\mathbf{x}_k = \mathbf{w}_k s_k + \mathbf{Q}_k \mathbf{a}_k \tag{32}$$

Burada s_k iletilmek istenen mesaj bilgisini içeren $\mathbb{E}\left\{|s_k|^2\right\} \leq P_s$ gücündeki sinyali belirtmektedir. $\mathbf{w}_k \in \mathcal{C}^{N_t \times 1}$ ise verici tarafındaki hüzmeleme vektörüdür. $\mathbf{a}_k = [a_1, a_2, \ldots, a_{N_t}]^T$ rasgele Gaussian dağılımlı vektör olup $\mathbb{E}\{||\mathbf{a}||^2\} \leq P_a$ gücüne sahip yapay gürültüdür (AN). $\mathbf{Q}_k \in \mathcal{C}^{N_t \times N_t}$, AN altuzayını oluşturan birim dik sütunlu AN vektörüdür. Hem $\mathbf{w}_k$ hem de $\mathbf{Q}_k$ Alice'deki yetkili kullanıcının mevcut kanal durum bilgisine göre belirlenir.

Burada P, toplam gücü ifade etmekte olup bilgi sinyalinin gücü olan P_s ve yapay gürültünün gücü olan P_a'nın toplanması ile elde edilmektedir. $P_s = \alpha P$ ve $P_a = \frac{1-\alpha}{N_t - 1} P$ olarak tanımlanmaktadır. Ayrıca α parametresi kanal koşul bilgisini ifade etmektedir ve değeri $(0, 1)$ aralığındadır. α'nın artması ile bilgi sinyaline ayrılan güç artarken, yapay gürültüye ayrılan güç azalmaktadır. Bu durum güvenlik kapasitesini etkilemektedir. Vericideki farklı kanal durum bilgisinin (tam ya da nicemsel) mevcudiyetine göre α parametresinin değeri optimal kanal güvenlik kapasitesini

sağlayacak şekilde seçilmelidir.

Yetkili kullanıcı ve gizli dinleyici tarafından alınmış sinyaller sırasıyla aşağıda ifade edilmiştir:

$$y_k = \mathbf{h}_k^H \mathbf{w}_k s_k + \mathbf{h}_k^H \mathbf{Q}_k \mathbf{a}_k + n_k, \tag{33}$$

$$\mathbf{y}^e = \mathbf{H}^e \mathbf{w}_k s_k + \mathbf{H}^e \mathbf{Q}_k \mathbf{a}_k + \mathbf{n}^e, \tag{34}$$

Burada $\mathbf{h}_k \in \mathcal{C}^{N_t \times 1}$ ve $\mathbf{H}^e \in \mathcal{C}^{N_e \times N_t}$ sırasıyla k. Bob'un kanalı ve Eve'in kanalı olup ortalaması sıfır ve varyansı 1 olan Gauss dağılımı ile modellenir. Bu modelde, gözönünde bulundurulan zaman çerçevesinde kanalın sabit olduğu sahip olduğu ve bir sonraki zaman çerçevesinde de bir önceki zaman çerçevesinden bağımsız olarak değiştiği varsayılmıştır. n_k ise Bob'daki ortalaması 0, varyansı σ^2 olan karmaşık toplamsal beyaz Gauss gürültüsünü (AWGN) ifade etmektedir. Bunun yanı sıra, $\mathbf{n}^e$'nin her bir elemanı da ortalaması 0, varyansı σ^2 olan Eve'deki AWGN'ye karşılık gelmektedir.

Bob'un CDI değerinin, $\mathbf{g}_k = \frac{\mathbf{h}_k}{\|\mathbf{h}_k\|}$ nicemlenmiş ve mükemmel bir şekilde Alice'de bilindiği durumları gözönüne alınmıştır. Bob'un CQI değerinin, $\|\mathbf{h}_k\|$, mükemmel bir şekilde Alice'de bilindiği varsayılmıştır.

Hüzmeleme vektörü $\mathbf{w}_k = \mathbf{g}_k$ olarak verilmiştir. $\mathbf{Q}_k$'nin sütunları ise $\mathbf{g}_k$'nin boş uzayı için birim dik doğru oluşturacak şekilde seçilmiştir. Bu ilişki $\mathbf{g}_k^H \mathbf{Q}_k = 0_{1 \times N_t}$ olarak tanımlanabilir.

Vericideki tam kanal durum bilgisi ile ulaşılabilecek güvenlik kapasitesi değeri şu şekilde hesaplanır:

$$C = \max\left\{\mathbb{E}\left\{\log_2\left(1 + SNR_k\right)\right\} - \mathbb{E}\left\{\log_2\left|\mathbf{I} + SNR^e\right|\right\}, 0\right\}^+, \tag{35}$$

Burada SNR_k ve SNR^e sırasıyla Bob'un ve Eve'in sahip olduğu ani SNR değerlerine karşılık gelmektedir ve bu değerler sırasıyla aşağıda verilmiştir:

$$SNR_k = \alpha\gamma \left\|\mathbf{h}_k\right\|^2 \tag{36}$$

$$SNR^e = \alpha(\mathbf{H}_e\mathbf{g}_k)^H \left(\frac{\sigma_e^2}{P}\mathbf{I} + \frac{(1-\alpha)}{N_t - 1}(\mathbf{H}_e\mathbf{Q}_k)(\mathbf{H}_e\mathbf{Q}_k)^H\right)^{-1} (\mathbf{H}_e\mathbf{g}_k) \tag{37}$$

burada $\gamma = \frac{P}{\sigma^2}$ yetkili kullanıcının sahip olduğu ortalama SNR'dır.

4.1.1 Kanalı nicemlenmiş yetkili kullanıcı durumu

Nicemlenmiş CDI durumunda, Alice tarafından iletilmiş sinyal,

$$\mathbf{x}_k = \hat{\mathbf{g}}_k s_k + \hat{\mathbf{Q}}_k \mathbf{a}_k, \tag{38}$$

olarak yazılabilir. Burada $\hat{\mathbf{g}}_k$ RVQ kullanılarak nicemlenmiş Bob'un CDI'ını ifade eder ve $\hat{\mathbf{Q}}_k$ nicemlenmiş CDI kullanılarak elde edilen vektördür.

Böylece yetkili kullanıcıda ve gizli dinleyicide elde edilen sinyaller sırasıyla,

$$y_k = ||\mathbf{h}_k||({\mathbf{g}_k}^H \hat{\mathbf{g}}_k)s_k + ||\mathbf{h}_k||({\mathbf{g}_k}^H \hat{\mathbf{Q}}_k)\mathbf{a}_k + n_k, \tag{39}$$

$$\mathbf{y}^e = \mathbf{H}^e \hat{\mathbf{g}}_k s_k + \mathbf{H}^e \hat{\mathbf{Q}}_k \mathbf{a}_k + \mathbf{n}^e. \tag{40}$$

olarak ifade edilir.

Nicemlenmiş CDI durumunda, k. Bob'a ait ani SNR değeri:

$$\hat{SNR}_k = \frac{\alpha ||\mathbf{h}_k||^2 |\mathbf{g}_k{}^H \hat{\mathbf{g}}_k|^2}{\frac{1-\alpha}{N_t-1} ||\mathbf{h}_k||^2 ||\mathbf{g}_k{}^H \hat{\mathbf{Q}}_k||^2 + \frac{1}{\gamma}}. \tag{41}$$

olarak verilir. RVQ özelliği kullanılarak ani SNR değeri aşağıdaki gibi yazılabilir:

$$\hat{SNR}_k = \frac{\alpha ||\mathbf{h}_k||^2 \cos\theta_k^2}{\frac{1-\alpha}{N_t-1} ||\mathbf{h}_k||^2 \sin\theta_k^2 + \frac{1}{\gamma}}. \tag{42}$$

Nicemlenmiş CDI durumunda, Eve'e ait ani SNR değeri:

$$\hat{SNR}^e = \alpha (\mathbf{H}^e \hat{\mathbf{g}}_k)^H \left(\frac{1-\alpha}{N_t - 1} (\mathbf{H}^e \hat{\mathbf{Q}}_k)(\mathbf{H}^e \hat{\mathbf{Q}}_k)^H \right)^{-1} (\mathbf{H}^e \hat{\mathbf{g}}_k) \tag{43}$$

Burada Eve'in kanalı ile ilgili herhangi bir bilgiye sahip olunmadığı için σ_e^2'in sıfır olduğu varsayılır. Böylece güvenlik kapasitesi açısından en kötü senaryo için sonuçlar elde edilir.

Nicemlenmiş CDI durumdaki güvenlik kapasitesi değeri aşağıdaki gibi gösterilir:

$$C^q = \max \left\{ \mathbb{E} \left\{ \log_2 \left(1 + \hat{SNR}_k \right) \right\} - \mathbb{E} \left\{ \log_2 \left| \mathbf{I} + \hat{SNR}^e \right| \right\}, 0 \right\}^+ \tag{44}$$

Yetkili kullanıcının kanal durum bilgisinin vericide tam olarak bilindiği durumun aksine, limitli CDI durumunda bir yapay gürültü sızıntısı (AN leakage) oluşmaktadır.$||\mathbf{h}_k||^2 |\mathbf{g}_k{}^H \hat{\mathbf{Q}}_k|^2$ terimi ile ifade edilen ve yetkili kullanıcının nicemlenmiş kanalının boş uzayından sızan gürültü güvenlik kapasitesi değerini düşürmektedir.

4.1.2 Kanalı bilinen gizli dinleyici durumu

Gizli dinleyicinin kanal bilgisinin Alice'de olması hem tek kullanıcılı hem de çok kullanıcılı sistemlerin fiziksel katman güvenliği açısından oldukça önemlidir. Pratik sistemlerde gizli dinleyici pasif olarak kabul edilmekle beraber gizli dinleyicinin kanal bilgisinin vericide bilindiği durum optimal performansların elde edilmesi ve gizli dinleyicinin kanalının bilinmediği durum ile karşılaştırılması açısından önemlidir.

Alice'de iki farklı yetkili kullanıcı seçim algoritması uygulanabilir. İlk seçim algoritmasında en yüksek norma sahip olan Bob seçilmektedir (En iyi Bob seçimi). Alice'deki ikinci seçim algoritmasında ise, bütün yetkili kullanıcılar arasından gizli dinleyici göre en iyi yetkili kullanıcı seçilmektedir. Bu aşamada en iyi kriteri ile gizli dinleyicinin en az bilgi alabileceği yani en yüksek güvenlik kapasitesini açığa çıkaracak Bob seçilmektedir (Optimal Bob seçimi).

Bob ve Eve'de alınan sinyaller sırasıyla aşağıdaki gibi tanımlanır:

$$y_k = \mathbf{h}_k^H \mathbf{x}_k + n_k, \tag{45}$$

$$\mathbf{y}^e = \mathbf{H}^e \mathbf{x}_k + \mathbf{n}^e, \tag{46}$$

Alice'de seçilmiş olan $k.$ yetkili kullanıcıya iletilen sinyal $\mathbf{x}_k = \mathbf{w}_k s_k$ olarak ifade edilmekte olup sinyalinin gücü ise $\mathbb{E}\{||\mathbf{x}||^2\} \leq P$ dir. Bu sistem modelinde Bob ve Eve'e eşit güç dağılımı yapıldığı varsayılmaktadır.

Gizli dinleyicinin kanal durum bilgisinin bilindiği durumda iki farklı şekilde hüzmeleme vektörü elde edilir. İlk yöntem, GSVD (Generalized singular value decomposition) dayalı olup $\mathbf{w}_k = \Psi_{max}$ olarak seçilir. Burada en yüksek özdeğer vektörü şu şekilde elde edilir:

$$\lambda_{max}(\mathbf{I} + P\mathbf{h}_k(\mathbf{h}_k)^H, \mathbf{I} + P(\mathbf{H}^e)^H\mathbf{H}^e) = \max_{\Psi \in C^{N_t}} \frac{\Psi^H(\mathbf{I} + P\mathbf{h}_k(\mathbf{h}_k)^H)\Psi}{\Psi^H(\mathbf{I} + P(\mathbf{H}^e)^H\mathbf{H}^e)\Psi}. \tag{47}$$

Güvenlik kapasitesi değeri:

$$C^p = \left\{\log(\lambda_{max}(\mathbf{I} + P\mathbf{h}_k(\mathbf{h}_k)^H, \mathbf{I} + P(\mathbf{H}^e)^H\mathbf{H}^e))\right\}^+ \tag{48}$$

olarak hesaplanır.

İkinci yöntemde ise ZFBF (Zero Forcing Beamforming) dayalı algoritma uygulanabilir.

$$\mathbf{W} = \mathbf{H}^H(\mathbf{H}\mathbf{H}^H)^{-1} \tag{49}$$

Burada birleşik kanal matrisi:

$$\mathbf{H} = [\mathbf{h}_k \quad \mathbf{H}^e]^H \tag{50}$$

Burada $\mathbf{H}$ Alice tarafından seçilmiş kullanıcının ve gizli dinleyici olarak davranan kullanıcının kanal durum bilgisini içermektedir. $\mathbf{w}_k$ ise $\mathbf{W}_k$'nin normalize edilmiş k. sütununa karşılık gelmekte olup $||\mathbf{w}_k|| = 1; \forall k$ şeklinde normalize edilmiştir.

Kanalın mükemmel bilindiği durumda $|\mathbf{h}_k^H\mathbf{w}_j| = 0$ eşitliği $k \neq j$ için sağlanmaktadır. Böylece seçilmiş kullanıcının hüzmeleme vektörü $\mathbf{w}_k$, gizli dinleyicinin kanalı dik olduğundan, tam kanal durum bilgisi vericide mevcut olursa gizli dinleyicinin bilgi alması tamamen engellenebilmektedir. Nicemlenmiş kanal durum bilgisi durumunda ise güvenlik kapasitesinde gizli dinleyicinin bilgi alması tamamıyle önlenemediğinden bir bilgi sızıntısı oluşur ve güvenlik kapasitesinde düşüş meydana gelir.

4.1.3 Benzetim Sonuçları

Tek gizli dinleyici durumu: Bu kısımda elde edilen benzetim çalışmalarında, baz istasyonundaki anten sayısı $N_t = 2$ olarak seçilmiştir [119]. $\mathcal{T}_1$ kriteri için eşik değeri γ_{th}, teorik olarak bir hücre içindeki ortalama kullanıcı sayısı $\bar{K} = 4$, olacak şekilde hesaplanmıştır. Kullanıcı sayıları $K = [10, 20, 30, 40, 50]$ için uygun olan eşik değerleri $\gamma_{th} = [2, 3, 3.5, 3.9, 4.15]$ olarak hesaplanmıştır. Bu eşik değerlerine göre $\mathcal{U}_1$ kümesi elde edilmiş, RVQ tabanlı kod kitapçığı ile nicemlenmiş ve B bit kullanılarak Alice'e iletilmiştir.

Şekil 9'de, kanal koşul parametresinin güvenlik kapasite değerine etkisini gösterilmektedir. Vericide kanal durum bilgisinin tam olduğu durum için en yüksek güvenlik kapasitesi değeri,

bilgi içeren sinyal ile yapay gürültü sinyaline eşit oranda güç ayrıldığı zaman elde edilir. Şekilden de görüleceği üzere, yetkili kullanıcının kanalı hakkındaki bilgimiz azaldıkça, yapay gürültü sinyaline ayrılan güç azalmalıdır. Yetkili kullanıcının kanal bilgisinin vericide limitli olması, bu kullanıcının yapay gürültüden negatif yönde etkilenmesine neden olmaktadır. Bu durum da bir bilgi sızıntısına yol açabilmektedir. Baz istasyonundaki kanal durum bilgisinin niteliğine göre, yapay gürültü sinyali ile bilgi sinyali arasındaki güç, güvenlik kapasitesini maksimuma çıkaracak şekilde verici tarafından ayarlanmalıdır. Güvenlik kapasitesi sonuçlarını karşılaştırmak için kanal koşul parametresi 0.5 olarak seçilmiştir ve bu durum yapay gürültü ile bilgi içeren sinyale eşit oranda güç ayrılmasına karşılık gelmektedir.

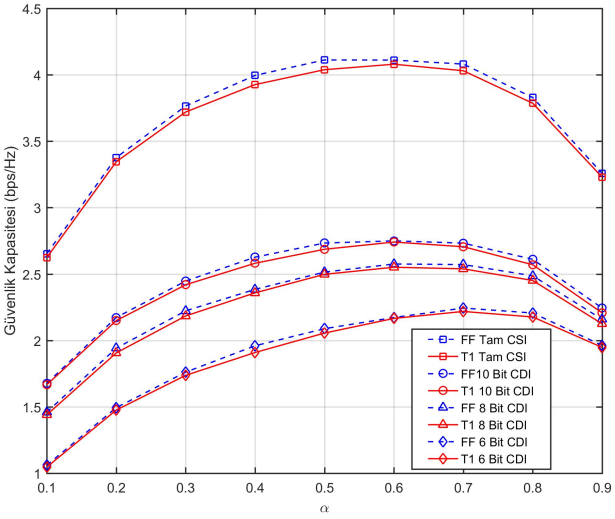
Şekil 10'de gösterildiği üzere, $\mathcal{T}_1$ kriteri uygulanmış sistemin güvenlik kapasite değeri, bütün yetkili kullanıcıların Alice'e kanal durum bilgilerini gönderdiği durumunu oldukça yakından takip etmektedir.$\mathcal{T}_1$ kriteri sayesinde güvenlik kapasitesi değerinde herhangi bir kayıp olmadan sistem yükü önemli ölçüde azaltılmıştır. Kullanıcı sayısına göre sistem yükündeki yüzdelik azalma 60 ile 90 arasında değişmektedir.

Birden fazla gizli dinleyici durumu: Bu kısımda elde edilen benzetim çalışmalarında, baz istasyonundaki anten sayısı $N_t = 4$ olarak seçilmiştir. $\mathcal{T}_1$ kriteri için eşik değeri γ_{th}, teorik olarak bir hücre içindeki ortalama kullanıcı sayısı $\bar{K} = 4$, olacak şekilde hesaplanmıştır. Kullanıcı sayıları $K = [10, 20, 30, 40, 50]$ için uygun olan eşik değerleri $\gamma_{th} = [4.15, 5.5, 6.2, 6.67, 7.0]$ olarak hesaplanmıştır. Bu eşik değerlerine göre $\mathcal{U}_1$ kümesi elde edilmiş, RVQ tabanlı kod kitapçığı üretilmiş ve B bit kullanılarak Alice'e iletilmiştir.

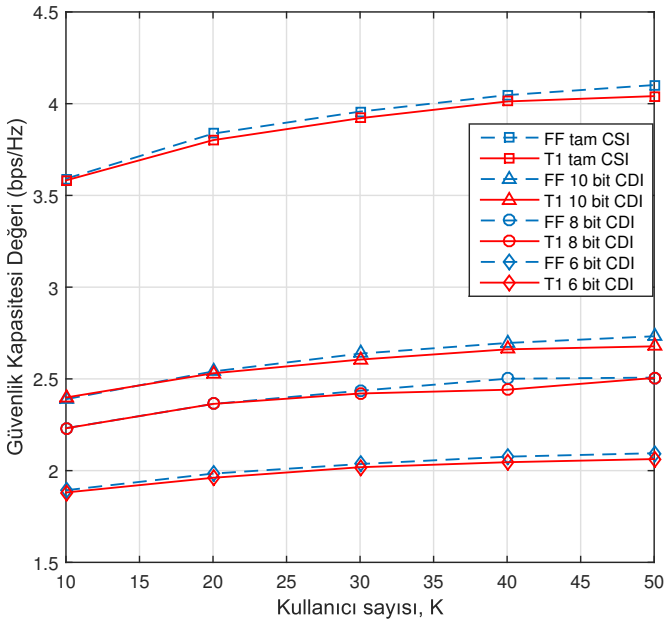
Şekil11 ve Şekil12'de ise, gizli dinleyicinin CSI'ının ve anten sayısının güvenlik kapasitesine etkisi, her iki durum için en iyi α değeri ile analiz edilmiştir. Vericide kullanıcıların CSI'ları mükemmel bir şekilde bilindiğinde, $N_t \geq N_e + 1$ için güvenlik kapasitesinin SNR ile sınırsız arttırılabileceği gözlemlenmiştir.

Tam geri besleme olarak bahsedilen durum, bütün kullanıcıların CSI'larını vericiye geri besleme kanalı ile iletmesine karşılık gelmektedir. Beklenildiği üzere, yüksek miktarda nicemleme biti kullanımı daha yüksek güvenlik kapasitesine ulaşmamızı sağlamaktadır. Gizli dinleyicinin kanal bilgisinin vericide mevcut olmadığı koşullarda, gücün bir kısmı dinleyicinin algısını bozmak için yapay gürültü sinyali oluşturulmasına ayrılmaktadır. En iyi güç dağıtım parametresi α, kullanıcıların kanal bilgilerinin nicemleme hatasından ne kadar etkilendiğine bağlı olarak değişmektedir. Tam geri besleme durumunda $B = 12$ ve $K = 50$ için, toplam geri besleme yükü $50 \times 12 = 600$ bit kullanımıdır. Eğer $\mathcal{T}_1$ kriteri kullanılırsa, ortalama sadece 4 kullanıcı CSI'ını vericiye iletmekte ve geri besleme yükü $4 \times 12 = 48$ bit kullanımına düşmektedir. Ayrıca, $\mathcal{T}_1$ kriteri kullanıldığında tam geri besleme durumuna nazaran güvenlik kapasitesinde bir düşüş oluşmamaktadır. Öte yandan, geri besleme yükünde ortalama kullanıcı sayısı K'ya bağlı olarak, $\%60 - \%92$ arasında değişen bir azalma gözlemlenmektedir.

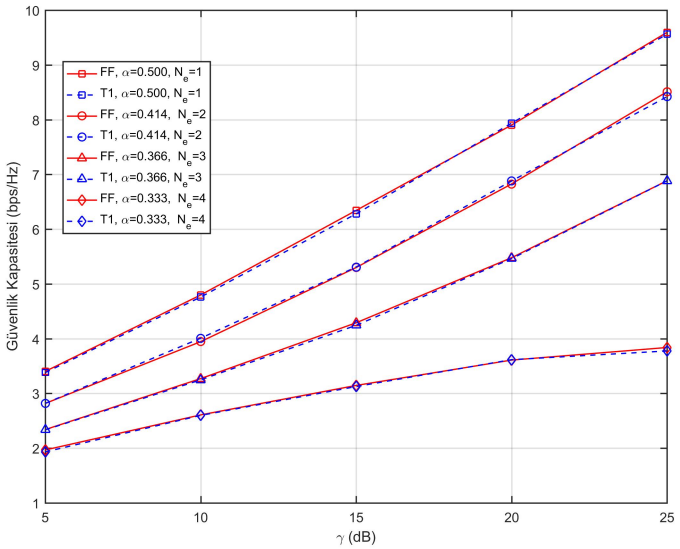
Şekil 13'da ise gizli dinleyicinin CSI'ının elde edilebildiği koşullarda, güvenlik kapasitesi kullanıcıdaki farklı nicemleme biti sayıları için elde edilmiştir. Sonuçlara göre, SNR'daki artış güvenlik kapasitesinde bir kayba yola açmaktadır. Gizli dinleyici kullanıcılardan daha fazla sayıda antene sahip olduğu için, hüzmelemenin yönü en iyi yönden sapmaktadır. Bu sonuç, CSI'ın mükemmel olarak elde edilebiliği durumla tam bir zıtlık içerisindedir.



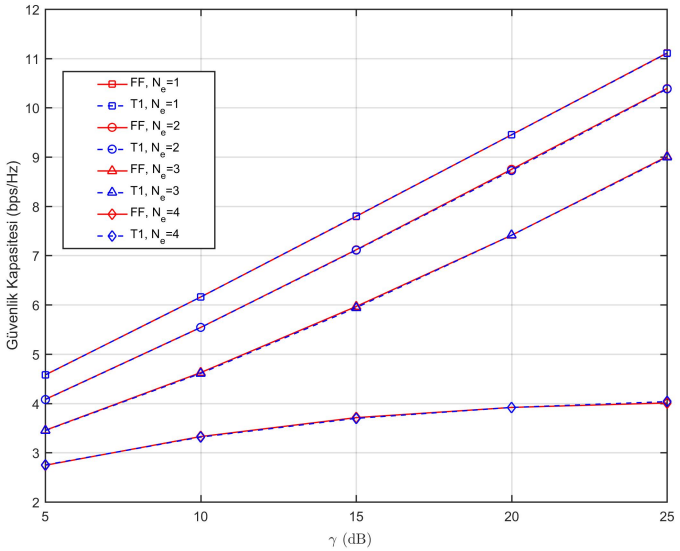
Şekil 9: Tam geri besleme (FF) durumu ve $\mathcal{T}_1$ kriterinin (T1), $\gamma = 10$dB ve K=50 için kanal koşul parametresine göre karşılaştırılması



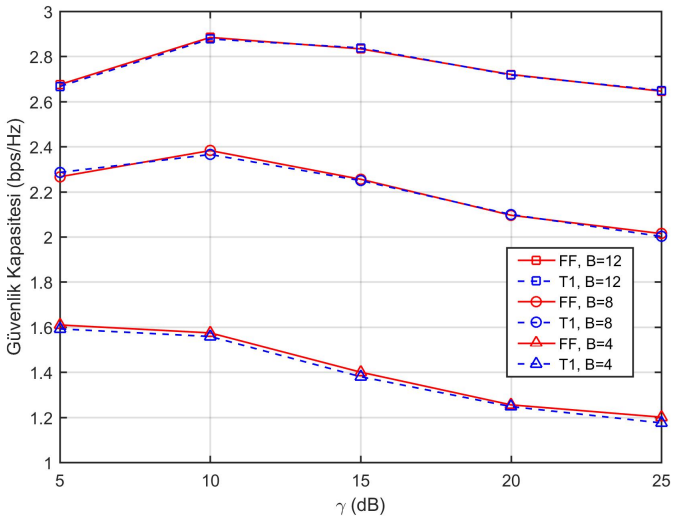
Şekil 10: Tam geri besleme (FF) durumu ve $\mathcal{T}_1$ kriterinin (T1), $\gamma = 10$dB ve $\alpha = 0.5$ için karşılaştırılması



Şekil 11: Gizli dinleyicinin CSI bilinmediği ve yetkili kullanıcıların CSI'larının mükemmel bilindiği durumunda güvenlik kapasitesinin γ'ya göre $K = 50$ ve farklı N_e'ler için karşılaştırılması.

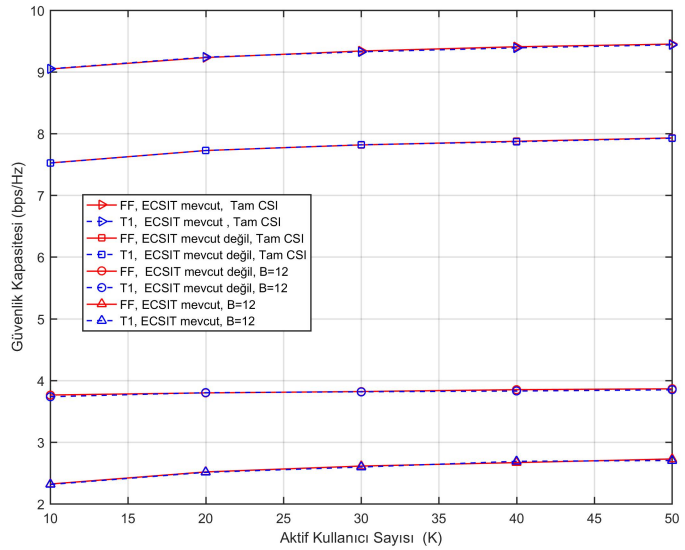


Şekil 12: Gizli dinleyicinin ve yetkili kullanıcıların CSI'larının mükemmel bilindiği durumunda, güvenlik kapasitesinin γ'ya göre $K = 50$ ve farklı N_e'ler için karşılaştırılması



Şekil 13: Gizli dinleyicinin ve yetkili kullanıcıların CSI'larının nicemlenmiş halinin vericide mevcut olduğu durumda, güvenlik kapasitesinin γ'ya göre karşılaştırılması $K = 50$, $N_e = 2$.

Şekil 14'de, vericide gizli dinleyicinin CSI'nın bulunduğu ve bulunmadığı durumlar için tam geri besleme ve $\mathcal{T}_1$ kriterleri kullanılarak kısıtlı geri besleme bağında karşılaştırılmıştır. Kullanıcının ve gizli dinleyicnin CSI'ı vericide mükemmel bir şekilde bilindiği durumda, gizli dinleyicinin kullanıcıya yollanan gizli mesajı elde etmesi mümkün olmamaktadır. Vericide gizli dinleyicinin bilgisi bulunmadığında ve kullanıcının kanal bilgisi nicemlenmiş bir şekilde mevcut olduğu durumda, nicemleme bit sayısı ve aktif kullanıcı sayısına bağlı olarak kayda değer bir güvenlik kapasitesi değeri elde edilebilir.



Şekil 14: Vericideki farklı CSI durumlarına göre güvenlik kapasitesi aktif kullanıcı sayısına göre karşılaştırılması. $\gamma = 20$dB.

4.2 Durağan olmayan kanallar güvenli MISO sistem modeli

Bu bölümde durağan olmayan kanal modeline sahip yetkili kullanıcının kanal durum bilgisinin vericiye iletilmesi aşamasında nicemlenmesi için diferansiyel kod kitapçığı kullanılmıştır. Bu kanal modelinde kanalın bir önceki zaman çerçevesi ile ilintili olduğu durum incelenmiştir. Tek bir gizli dinleyici olduğu ve gizli dinleyicinin kanal durum bilgisinin bilinmediği durum sunulmuştur.

Diferansiyel kod kitapçığı, sönümlü kanalların zamansal ilintisini (korelasyon) kullanarak sistem performansını arttırmayı hedefleyen bir kısıtlı geri besleme yöntemidir. Bu yöntemde, vericinin hüzmeleme vektörünün bir zaman birimi önceki durumunu bildiği ve kanalın zamanda ilintili olduğu varsayılır. Vericideki eski kanal yön bilgisinin ve mevcut andaki normalize edilmiş kanal vektörünün yönsel değişimleri kullanılarak yeni hüzmeleyici vektör oluşturulur. Ardışık zaman aralıklarında gerçekleşen bu yönsel değişimler Grassmann manifoldunun kesellerine (geodesics) karşılık gelmektedir.

Bu bölümde ele aldığımız sistem modeli bir verici, bir alıcı ve gizli dinleyiciden oluşmaktadır. Alice'de $N_t \geq 2$, Bob'da $N_r = 1$ ve Eve'de $N_e \geq 2$ anten bulunmaktadır. Kullanıcıya yollanmak istenen mesajlar, gizli dinleyici tarafından çözülmesini engellemek adına, yapay gürültü ile maskelenmiştir. Yani τ anındaki mesaj sinyali,

$$\mathbf{x}_\tau = \mathbf{w}_\tau s + \mathbf{Q}_\tau \mathbf{a} \tag{51}$$

şeklinde ifade edilebilir. Burada s asıl iletilmek istenen bilgi sinyali iken $\mathbf{a}$ yapay gürültü vektörüdür. Ayrıca, $\mathbf{w}_\tau$ diferansiyel kod kitapçığı yardımıyla verici tarafından τ anında oluşturulan hüzmeleyici vektördür. $\mathbf{Q}_\tau$ matrisi ise $\mathbf{w}_\tau$'nun boş uzayında oluşturulmuş yapay gürültünün hüzmeleyici vektörüdür. $\mathbf{Q}_\tau$ boş uzayda oluşturulmasının sebebi, kullanıcının bu gürültüden etkilenmesini olabildiğince azaltmaktır.

Kullanıcı ve gizli dinleyici tarafından alınan sinyaller ise,

$$y_\tau = \mathbf{h}_\tau^H \mathbf{w}_\tau s + \mathbf{h}_\tau^H \mathbf{Q}_\tau \mathbf{a} + n_\tau \tag{52}$$

$$\mathbf{y}_\tau^e = \mathbf{H}^e \mathbf{w}_\tau s + \mathbf{H}^e \mathbf{Q}_\tau \mathbf{a} + \mathbf{n}_\tau^e \tag{53}$$

Kullanıcının kanal vektörü $\mathbf{h}_\tau \in \mathcal{C}^{N_t \times 1}$ ile gösterilirken, $\mathbf{H}^e \in \mathcal{C}^{N_e \times N_t}$ gizli dinleyicinin kanal vektörüne karşılık gelmektedir. Burada gizli dinleyicinin kanalı $\mathcal{CN}(0,1)$ modellenmiştir. Yetkili kullanıcıdaki ve gizli dinleyicideki karmaşık toplanır beyaz Gauss gürültüleri (AWGN) sırasıyla $\mathcal{CN}(0,\sigma^2)$ ve $\mathcal{CN}(0,\sigma_e^2)$ dağılımlarına sahiptir.

Diferansiyel kod kitapçığı kullanılarak oluşturulan kod kitapçığı ile elde edilen hüzmeleme vektörlerine göre yetkili kullanıcıda ve gizli dinleyicide τ anında elde edilen SNR değerleri sırasıyla Eve2in kanalı ile hiçbir bilgi bilinmediği durumda

$$SNR_\tau = \frac{\alpha |\mathbf{h}_\tau^H \mathbf{w}_\tau|^2}{\frac{1-\alpha}{N_t-1} |\mathbf{h}_\tau^H \mathbf{Q}_\tau|^2 + \frac{1}{\gamma}} \tag{54}$$

$$SNR_\tau^e = \alpha(\mathbf{H}^e\mathbf{w}_\tau)^H \left(\frac{1-\alpha}{N_t-1}(\mathbf{H}^e\mathbf{Q}_\tau)(\mathbf{H}^e\mathbf{Q}_\tau)^H\right)^{-1}(\mathbf{H}^e\mathbf{w}_\tau) \tag{55}$$

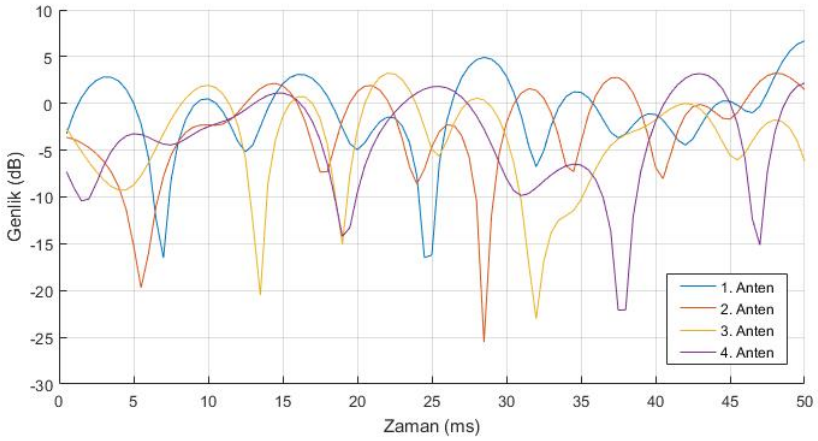
şeklinde yazılabilir.

Böylece elde edebileceğimiz güvenlik kapasitesi

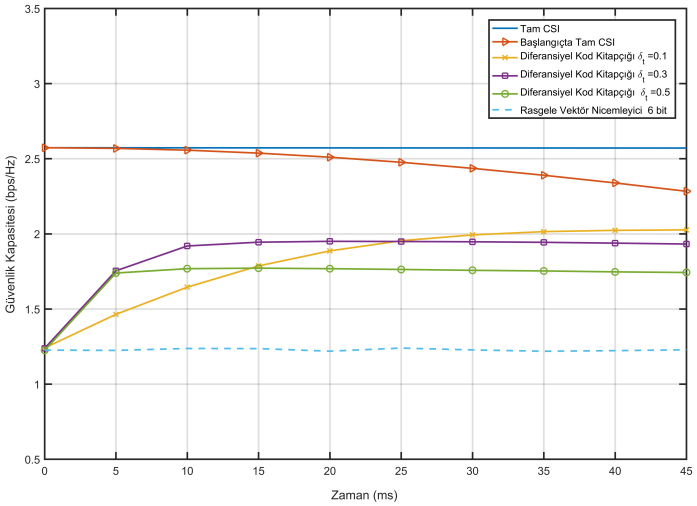
$$C_\tau = \max\{(\log_2(1+SNR_\tau) - \log_2(1+SNR_\tau^e)), 0\}^+ \tag{56}$$

olarak bulunur.

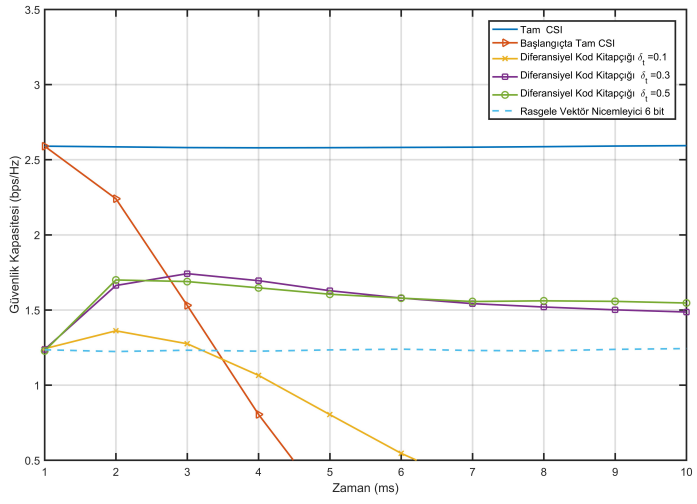
Benzetim Sonuçları Diferansiyel kod kitapçığı kullanılan sistemin güvenlik kapasitesi performansı Monte Carlo benzetimleri ile sunulmuştur. Benzetimler için vericideki anten sayısı $N_t = 4$ seçilirken, kullanıcıdaki ve gizli dinleyicideki anten sayıları sırasıyla $N_r = 1$ ve $N_e = 2$'dir. Rayleigh sönümlü kanal Jakes modeline dayanılarak tasarlanmıştır. Kanal ilinti parametresi $z = J_0(2\pi f_D T)$ ile hesaplanır. J_0 birinci tipten sıfırıncı derece Bessel fonksiyonuna karşılık gelir. Maksimum Doppler frekansı $f_D = \frac{vf_c}{c}$, $f_c = 2.4$ GHz, $T = 5$ ms olarak verilmiştir. Benzetim çalışmalarında $v = 0.45km/sa$, $v = 2.25km/sa$ ve $v = 4.5km/sa$ olarak seçilmiştir. Bu değerlere karşılık gelen $f_D = 1, 5, 10$ Hz olup ilinti değerleri $z = 0.9998, 0.9938, 0.9755$'dır. Şekil 15'de kanal genlik değerinin zamanla değişimi $f_D = 5$ için gösterilmiştir. Şekil 16 ve Şekil 17'da farklı hız değerlerinde $\gamma = 10$dB için güvenlik kapasitesi sonuçları gösterilmiş ve diferansiyel kod kitapçığının RVQ göre çok daha iyi sonuçlar verdiği gözlemlenmiştir. İlaveten diferansiyel kod kitapçığının kanalın zamanla değişimi takip ettiği ve güvenlik kapasitesinin hemen hemen aynı kaldığı gösterilmiştir.



Şekil 15: Kanal genlik değerinin zamanla değişimi.



Şekil 16: Zamana göre güvenlik kapasitesi sonuçları, $\gamma = 10$dB, $f_D = 1$Hz.



Şekil 17: Zamana göre güvenlik kapasitesi sonuçları, $\gamma = 10$dB, $f_D = 10$Hz.

4.3 Güvenli MISO-OFDM sistemi

Yeni nesil haberleşme sistemlerinde kullanılan çok antenli yapılar ile uzayda iletim seçiciliği sağlanarak güvenlik çözümleri geliştirilebilir. Bu bölümde, MISO-OFDM tabanlı kablosuz haberleşme sistemlerinde frekans ve uzaydaki seçiciliği kullanılarak frekans-uzamsal (frequency-temporal) kanal imzaları çıkartmak ve bu imzalara bağlı özgün ve pratikte kullanılabilir bir fiziksel katman güvenliği geliştirilmiştir. Bu doğrultuda durağan kablosuz kanal yapıları göz önünde bulundurulmuştur. Alıcıda verinin güvenliğinin sağlanmasına temel teşkil edecek sistemin tasarımı, alttaşıyıcı kümelerinin sınıflandırılması, her alttaşıyıcı kümesi için kablosuz kanalın faz bilgisinin güvenliği ön planda tutan kriterlere göre tasarlanmış kod kitapçığı kullanılarak nicemlenmesi ve bilginin gizli alıcılar tarafından sezinlenme olasılığı azaltmak için hüzmeleme vektörünün belirlenmesi ile yapılmıştır.

4.3.1 Sistem Modeli

Gözönüne alınan sistemde N alttaşıyıcı, tek antenli tek gizli dinleyici (Eve), tek antenli yetkili dinleyici (Bob), N_t verici antenli baz istasyonu (Alice) bulunmaktadır. Alice, Bob'a gizli mesajlar iletme istediğinden AN ile Eve'e karışım oluşturmaktadır. Alice'de Eve'in kanal durumu ile ilgili herhangi bir bilgi bulunmamaktadır ve Bob'un kanal durum bilgisi limitli geri besleme kanalı üzerinden Alice'e gönderilir.

Hem alıcı hem de verici tarafında bilinen pilot semboller yardımıyla vericide kanal kestirimi yapılır. Pilot sembollerinin kanal kestiriminde kullanılması sebebiyle bit hata oranlarının düşük olması önemlidir. Bu yüzden Binary modülasyon teknikleri (örneğin BPSK) kullanılarak gönderilmiştir. Frekans ilinti faktörü kablosuz kanala yapısına göre önceden bilindiği için her bir alttaşıyıcı kümesinin kaç adet alttaşıyıcı içereceği önceden belirlenir.

Hem alıcı hem de verici tarafında alttaşıyıcılar kablosuz kanalın frekans ilintisi faktörlerine göre kümelenirler. Buradaki amaç aynı nicemleme değerlerine sahip alttaşıyıcı sayısını en aza indirerek birbirinden farklı güvenlik imzaları oluşturmaktır. Alttaşıyıcı kümeleme işlemi

$$m = (q-1)N_Q + \arg \min_{1 \le i \le N_Q} \{||\mathbf{H}_{(q-1)N_q+i}||^2\} \tag{57}$$

ile gerçekleştirilir.

Kümelenen alttaşıyıcıları temsil eden bir alttaşıyıcı ile

$$\mathbf{H}_q = \mathbf{H}_m \tag{58}$$

seçilir. Burada $\mathbf{H}_m$ m. alttaşıyıcısına ait $N_t \times 1$ boyutunda Bob'un kanal durum vektörüdür. $N_Q = N/Q$ alttaşıyıcı kümesindeki alttaşıyıcı sayısını ve Q toplam alttaşıyıcı küme sayısını temsil eder.

Herbir alttaşıyıcı kümesi için gönderilen sinyal:

$$\mathbf{X}_q = \mathbf{W}_q S_q + \mathbf{Q}_q \mathbf{a}_q, \tag{59}$$

Burada S_q gönderilen veridir ve $\mathbb{E}\{|S_q|^2\} \leq \frac{P_s}{Q^a}$ gücündedir. Q^a haberleşme sağlanan toplam aktif alttaşıyıcı kümesidir. $\mathbf{W}_q \in \mathcal{C}^{N_t \times 1}$ her bir alttaşıyıcı için hüzmeleme vektörüdür. $\mathbf{a}_q = [a_{q_1}, a_{q_2}, \ldots, a_{q_{N_t}}]^T$ vektörü q. alttaşıyıcı kümesi için AN'dir ve gücü $\mathbb{E}\{||\mathbf{a}_q||^2\} \leq P_a$. $\mathbf{Q}_q \in \mathcal{C}^{N_t \times N_t}$ ise AN hüzmeleme vektörüdür. $\mathbf{W}_q$ and $\mathbf{Q}_q$ Alice'deki Bob'un bilinen CSI göre hesaplanır. Burada güç paylaşımı $P_s = \alpha P$ ve $P_a = \frac{1-\alpha}{N_t - 1} P$ olarak yapılmakta olup $P = P_a + P_s$ toplam güç, α kanal koşul parametresidir.

Bob ve Eve'de alınan sinyaller sırasıyla:

$$Y_q = \mathbf{H}_q^H \mathbf{W}_q S_q + \mathbf{H}_q^H \mathbf{Q}_q \mathbf{a}_q + Z_q, \tag{60}$$

$$Y_q^e = (\mathbf{H}_q^e)^H \mathbf{W}_q S_q + (\mathbf{H}_q^e)^H \mathbf{Q}_q \mathbf{a}_q + Z_q^e, \tag{61}$$

Burada $\mathbf{H}_q \in \mathcal{C}^{N_t \times 1}$ ve $\mathbf{H}_q^e \in \mathcal{C}^{N_t \times 1}$ sırasıyla Bob ve Eve'in her alttaşıyıcı kümesi q'ya ait kanal vektörleridir. Frekans seçici kanalın frekans ortamındaki tepkimesidir. Z_q ve Z_q^e Bob ve Eve'deki AWGN'dur. Bu gürültüler sıfır ortalamalıdır ve sırasıyla σ^2 ve σ_e^2 varyanslara sahiptir.

Herbir alttaşıyıcı kümesi için Bob'un CDI $\mathbf{G}_q = \frac{\mathbf{H}_q}{\|\mathbf{H}_q\|}$ ve CQI değeri $\|\mathbf{H}_q\|$'dır. Hüzmeleme vektörü $\mathbf{W}_q = \mathbf{G}_q$ ve $\mathbf{G}_q^H \mathbf{Q}_q = 0_{1 \times N_t}$'dir.

Bob ve Eve'deki ani SNR:

$$SNR_q = \frac{\|\mathbf{H}_q\|^2 \frac{\alpha}{Q^a}}{\frac{1}{Q}\frac{1}{\gamma}}, \tag{62}$$

$$SNR_q^e = \frac{\left|(\mathbf{H}_q^e)^H \mathbf{W}_q\right|^2 \frac{\alpha}{Q^a}}{\left|(\mathbf{H}_q^e)^H \mathbf{Q}_q\right|^2 \frac{(1-\alpha)}{(N_t-1)Q^a} + \frac{1}{Q}\frac{1}{\gamma_e}}, \tag{63}$$

Burada Bob'un ortalama SNR değeri $\gamma = \frac{P}{\sigma^2}$olup Eve'in CSI hakkında herhangi bir bilgi sahibi olmadığımız için $\sigma_e^2 = 0$ olduğu varsayılmıştır.

Mükemmel CSI durumunda güvenlik kapasitesi:

$$R = \frac{1}{Q} \sum_{q=1}^{Q} \mathbb{E}\left\{\log_2\left(1 + SNR_q\right)\right\} - \mathbb{E}\left\{\log_2\left(1 + SNR_q^e\right)\right\} \tag{64}$$

şeklinde hesaplanır.

Her bir alttaşıyıcı kümesi için Bob'un CDI bilgisi nicemlenir ve her biri B bit olarak Alice'e iletilir. Bu durumda Bob'un SNR'ı aşağıdaki gibi ifade edilir:

$$\hat{SNR}_q = \frac{|(\mathbf{H}_q)^H \hat{\mathbf{G}}_q|^2 \frac{\alpha}{Q^a}}{|(\mathbf{H}_q)^H \hat{\mathbf{W}}_q|^2 \frac{1-\alpha}{(N_t-1)Q_a} + \frac{1}{Q}\frac{1}{\gamma}}, \tag{65}$$

Kanalın mükemmel bilindiği duruma göre $||\mathbf{H}_q||^2 |\mathbf{G}_q{}^H \hat{\mathbf{W}}_q|^2$ terimi sızıntıyı belirler ve güvenlik kapasitesi azalır.

Nicemlenmiş CDI durumunda Eve'in SINR aşağıdaki gibi ifade edilir:

$$\hat{SNR}_q^e = \frac{|(\mathbf{H}_q^e)^H \hat{\mathbf{G}}_q|^2 \alpha}{|(\mathbf{H}_q^e)^H \hat{\mathbf{W}}_q|^2 \frac{1-\alpha}{(N_t-1)}}. \tag{66}$$

Limitli geri besleme kanalı durumunda güvenlik kapasitesi

$$\hat{R} = \frac{1}{Q}\sum_{q=1}^{Q} \mathbb{E}\left\{\log_2\left(1+S\hat{N}R_q\right)\right\} - \mathbb{E}\left\{\log_2\left(1+S\hat{N}R_q^e\right)\right\} \tag{67}$$

4.3.2 Uzamsal imzaya dayalı güvenli haberleşme

Önerilen uzamsal imzaya dayalı güvenli haberleşme algoritmasının basamakları aşağıda verilmiştir:

- *Basamak 1: Karmaşık rasgele dik vektörlerin üretilmesi:*

  Her alttaşıyıcı kümesi q için, $N_t \times 1$ boyutunda N_t adet karmaşık rasgele dik vektör üretilmesi, $\boldsymbol{\phi}_{n,q,m}$ burada $n = 1, ..., N_t$, $q = 1, ..., Q$ ve $m = 1, ..., M$. Tüm bu vektörler hem Alice hem de Bob tarafında bilindiği varsayılmaktadır. Fakat gizli dinleyici tarafından bilinmemektedir.

- *Basamak 2: Alttaşıyıcı kümelenmesi:*

  Alttaşıyıcı kümeleri Basamak 1'de üretilen vektörler kullanılarak sınıflandırılır. Bu sınıflandırmayı yapmak amacıyla her alttaşıyıcı kümesi için kirişsel (chordal) uzaklığı ile ölçülür:

  $$(n_q^*, m_q^*) = \arg\min_{\forall n, \forall m} d^2(\mathbf{G}_q, \boldsymbol{\phi}_{n,q,m}), \forall q \tag{68}$$

  Burada $d^2(\mathbf{G}_q, \boldsymbol{\phi}_{n,q,m}) = 1 - |\mathbf{G}_q^H \boldsymbol{\phi}_{n,q,m}|^2$.

  Burada birden fazla küresel bölgeler oluşturularak alttaşıyıcılar kümelenir.

  $$\mathcal{Q}^r = \{q = 1, 2, ...Q : \mathbf{G}_q \in \bigcup_{m=1}^{M}\bigcup_{i=1}^{N_t} \mathcal{B}_\epsilon(\mathbf{G}_q, \boldsymbol{\phi}_{n,q,m}\}. \tag{69}$$

  Burada $\mathcal{B}_\epsilon(\mathbf{f}, \mathbf{o}) = \{\mathbf{f} \in \mathcal{O}^{N_t} : d_c^2(\mathbf{f}, \mathbf{o}) \leq \epsilon\}$.

  Buradaki amaç alttaşıyıcı kümelerinin hem frekans hem de uzamsal çeşitlilik özelliklerini açığa çıkararak sınıflandırma yapmaktır. Herhangi bir alttaşıyıcı kümesi herhangi bir sınıfta yer almadıysa o alttaşıyıcı kümesinden veri aktarımı yapılmaz.

- *Basamak 3: Döndürülmüş kod kitapçığı ile nicemleme:* Basamak 1'de üretilen her rasgele vektör ve her alttaşıyıcı kümesi için birbirinden farklı döndürülmüş kod kitapçığı üretilir.

  $$\mathbf{C}_{j,n,q,m}^{rot} = \mathbf{U}_{n,q,m}^{rot}\mathbf{C}_j^{\epsilon}; j = 1, ..., 2^B \tag{70}$$

  Burada $\mathbf{U}_{n,q,m}^{rot} = \boldsymbol{\phi}_{n,q,m}\mathbf{o}^{-1}$. Daha sonra her alttaşıyıcı kümesinin CDI'yı kendisine ait döndürülmüş kod kitapçığı kullanarak nicemlenir.

  $$q_j^{rot} = \arg\min_{1 \leq j \leq 2^B} d^2(\mathbf{G}_q, \mathbf{C}_{j,n_q^*,q,m_q^*}^{rot}) \tag{71}$$

Böylece kod kitapçığının tüm bölgeyi kapsaması yerine açısal olarak belli bir bölgeye odaklaması sağlanarak nicemleme hatası azaltılmış ve güvenlik için kanalın imza çeşitliliği arttırılmıştır. Tüm bu kod kitapçıkları hem alıcı hem de vericiye iletilir.

Alıcı tarafında alttaşıyıcı kümelerinin sınıflandırmalarına dayalı olarak üretilen kod kitapçıklarından uygun olan kod kitapçığı seçilir ve alttaşıyıcı kümesini temsil eden alttaşıyıcının kanal faz bilgisinin kirişsel (chordal) uzaklığı yöntemi ile nicemlenir ve CDI indeksi elde edilir. MISO-OFDM sistemlerinde frekans seçici bir kanal söz konusu olduğu için her alttaşıyıcı kümesi için farklı bir kod kitapçığı kullanımı ile kanalın hem frekans hem de uzamsal seçicilik özelliği açığa çıkarılırmıştır.

Daha sonra nicemlenmiş hüzmeleme vektörü,

$$\hat{\mathbf{G}}_q = \mathbf{C}^{rot}_{q_j^{rot},n_q^*,q,m_q^*} \tag{72}$$

ile elde edilir.

4.3.3 Benzetim Sonuçları

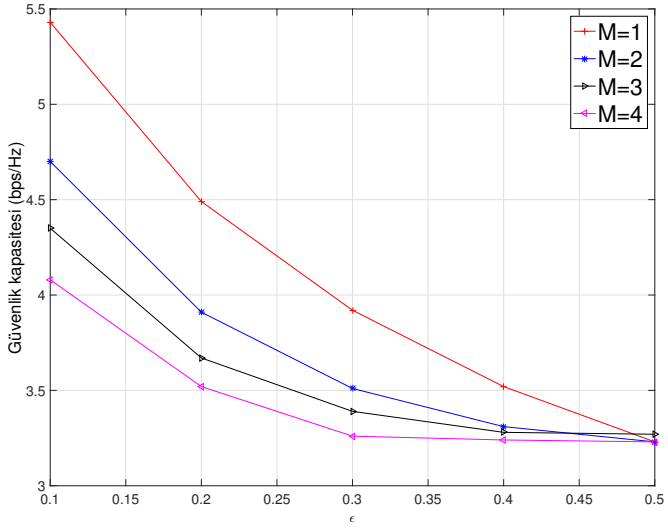
Benzetim sonuçları $N_t = 2$ verici antenli tek yetkili kullanıcı ve tek gizli dinleyici olan güvenli MISO-OFDM sistemi için elde edilmiştir. Kablosuz kanal 3GPP-TU modeline göre 3 km/saat hızı için taşıyıcı frekansı 2.4GHz için modellenmiştir. Toplam alttaşıyıcı kümesi $Q = 48$ olarak seçilmiştir.

Öncelikle ϵ ve M parametrelerinin güvenlik kapasitesi üzerindeki etkisi Şekil 18'de gösterilmiştir. Küçük ϵ değerleri için güvenlik kapasitesi M'den bağımsız olarak yüksektir. Bunun sebebi nicemleme hatasının azaltılmasıdır. Fakat bu durumda aktif alttaşıyıcı kümesi başına düşen güç artmaktadır. Çizelge 1'da gösterildiği gibi en iyi çözüm için $M = 2$ ve $\epsilon = 0.2$ seçilmiştir.

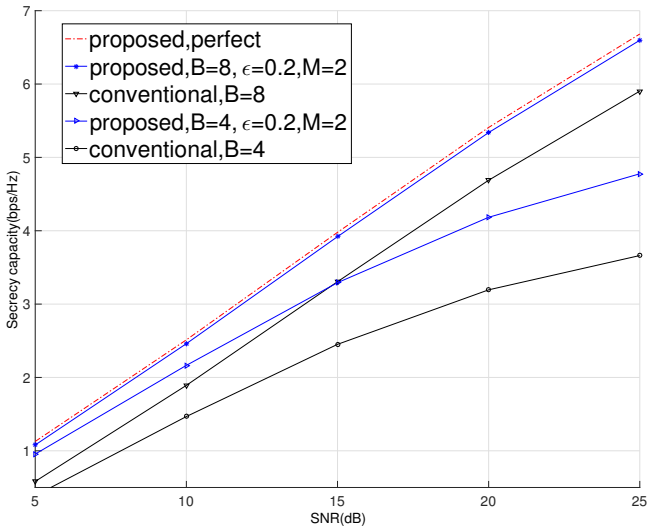
Çizelge 1: Ortalama aktif alttaşıyıcı küme sayısı

(ϵ, M)	Q^a	(ϵ, M)	Q^a	(ϵ, M)	Q^a	(ϵ, M)	Q^a
$(0.1, 1)$	10	$(0.1, 2)$	17	$(0.1, 3)$	23	$(0.1, 4)$	28
$(0.2, 1)$	18	$(0.2, 2)$	32	$(0.2, 3)$	38	$(0.2, 4)$	42
$(0.3, 1)$	29	$(0.3, 2)$	40	$(0.3, 3)$	45	$(0.3, 4)$	47
$(0.4, 1)$	38	$(0.4, 2)$	46	$(0.4, 3)$	48	$(0.4, 4)$	48
$(0.5, 1)$	48	$(0.5, 2)$	48	$(0.5, 3)$	48	$(0.5, 4)$	48

Şekil 19'de ise önerilen algoritma ile standart algoritma güvenli MISO-OFDM sistemleri için karşılaştırılmış olup önerilen algoritmasnın farklı SNR değerlerine göre yaklaşık 1 bps/Hz ile 1.5 bps/Hz değerleri arasında güvenlik kapasitesini arttırdığı gösterilmiştir.



Şekil 18: Farklı ϵ ve M değerleri için güvenlik kapasitesi, $B = 8$ ve $\rho = 15$dB.



Şekil 19: MISO-OFDM için güvenlik kapasitesi değerlerinin karşılaştırılması.

4.4 Güvenli çoklu kullanıcılı MISO sistemi

Kullanıcılar arasındaki karışım, klasik çoklu kullanıcı haberleşmesinde belirleyici bir role sahiptir. Güvenli haberleşmede ise, gizli dinleyicinin algısını olumsuz olarak etkilediğinden sisteme pozitif bir etkisi olabilir. Doğru M kullanıcı kombinasyonunun seçimi, güvenlik kapasitesi toplamını arttıracağından oldukça kritiktir. Bu sebeple, kullanıcı tarafında yarı-dik kullanıcı seçim algoritması ve özel kod kitapçığı tasarımının kullanılması önerilmiştir [120] . Böylece, özel kod kitapçığına göre kanallarını nicemlemiş ve kanal kalitesi eşik değerinden yüksek olan kullanıcılar kanal bilgilerini vericiye yollamaktadır. Bu kullanıcılar arasından vericide norm bilgileri kullanılarak M en iyi kullanıcı daha yüksek güvenlik kapasitesi toplamı elde etmek için seçilmektedir.

Bu bölümde, N_t antene sahip verici gizli mesajları seçilmiş M kullanıcıya göndermeyi amaçlamaktadır. M kullanıcı güvenli haberleşme için K aktif kullanıcı arasından seçilmiştir. Gizli dinleyicisi ise bu M kullanıcıya gelen mesajları dinlemektedir. Gizli dinleyicinin pasif olduğu ve kanal durum bilgisinin vericide bulunmadığı varsayılmıştır.

Vericide yollanan sinyal $\mathbf{x}$,

$$\mathbf{x} = \hat{\mathbf{W}}\mathbf{s}, \tag{73}$$

olarak ifade edilebilir. Burada $\mathbf{s} = [s_1, s_2, \ldots, s_M]$ gücü $\mathbb{E}\{||\mathbf{s}||^2\} \leq P$ olan bilgi sinyali vektörünü ifade ederken, $\hat{\mathbf{W}} = [\hat{\mathbf{w}}_1, \hat{\mathbf{w}}_2 \ldots, \hat{\mathbf{w}}_m, \ldots, \hat{\mathbf{w}}_M]$ vericideki hüzmeleyici matrisine karşılık gelmektedir. Hüzmeleyici matrisi $\hat{\mathbf{W}}$, ZFBF yöntemi kullanılarak, nicemlenmiş kanal durum bilgisinden elde edilmiş olup $\hat{\mathbf{W}} = \hat{\mathbf{H}}(\mathbf{M})^H(\hat{\mathbf{H}}(\mathbf{M})\hat{\mathbf{H}}(\mathbf{M})^H)^{-1}$ şeklinde oluşturulmaktadır. Kanal matrisi $\hat{\mathbf{H}}(\mathbf{M}) \in \mathcal{C}^{M \times N_t}$, seçilmiş kullanıcıların nicemlenmiş kanal vektörlerinden elde edilmiştir. Kanal vektörü $\mathbf{h}_m \in \mathcal{C}^{N_t \times 1}$, $\mathcal{CN}(0, \mathbf{I})$ ile modellenmiştir. Hüzmeleyici matrisi $\hat{\mathbf{W}}$'nin sütunları normalize edilmiştir ($||\hat{\mathbf{w}}_m|| = 1$). Kullanıcıların kanal durum bilgileri mükemmel bir şekilde elde edilemediği durumda CDI $\mathbf{g}_k = \frac{\mathbf{h}_k}{||\mathbf{h}_k||}$ ve CQI $||\mathbf{h}_k||$ nicemlenmiş halleri kullanılabilir. Bu çalışmada, CQI'nın vericide mükemmel bir şekilde bilindiği varsayılmaktadır. K aktif kullanıcının her biri, kendi kanal durum bilgisini önceden belirlenmiş 2^B uzunluğundaki kod kitapçığından birim normdaki kod sözcüklerini seçerek nicemlemektedir.

Böylece, $m.$ kullanıcıda alınan sinyal

$$y_{b_m} = ||\mathbf{h}_{b_m}||(\bar{\mathbf{h}}_{b_m}^H \hat{\mathbf{w}}_m)s_m + \sum_{j=1, j\neq m}^{M} ||\mathbf{h}_{b_m}||(\bar{\mathbf{h}}_{b_m}^H \hat{\mathbf{w}}_j)s_j + n_{b_m}, \tag{74}$$

olarak yazılabilir. Burada, n_{b_m} ortalaması sıfır ve varyansı σ^2 olan karmaşık toplanır beyaz Gaussian gürültüsüdür.

Gizli dinleyicide elde edilen $m.$ kullanıcının mesaj sinyali,

$$y_{e_m} = (\mathbf{h}^e)^H \hat{\mathbf{w}}_m s_m + \sum_{j=1, j\neq m}^{M} (\mathbf{h}^e)^H \hat{\mathbf{w}}_j s_j + n_e. \tag{75}$$

ve n_e ortalaması sıfır ve varyansı σ_e^2 olan karmaşık toplanır beyaz Gaussian gürültüsüdür.

m. kullanıcıdaki sinyal karışım-gürültü oranı (SINR)

$$\hat{SINR}_{b_m} = \frac{\frac{1}{M}||\mathbf{h}_{b_m}||^2|\bar{\mathbf{h}}_{b_m}^H \hat{\mathbf{w}}_m|^2}{\sum_{j=1,j\neq m}^{M} \frac{1}{M}||\mathbf{h}_{b_m}||^2|\bar{\mathbf{h}}_{b_m}^H \hat{\mathbf{w}}_j|^2+\frac{1}{\gamma}}, \tag{76}$$

olarak ifade edilir.

Gizli dinleyicideki m. kullanıcının mesajına karşılık gelen SINR

$$\hat{SINR}_{e_m} = \frac{\frac{1}{M}\ |(\mathbf{h}^e)^H \hat{\mathbf{w}}_m|^2}{\sum_{j=1,j\neq m}^{M} \frac{1}{M}\ |(\mathbf{h}^e)^H \hat{\mathbf{w}}_j|^2}. \tag{77}$$

Burada $\sigma_e^2 = 0$'dır.

Bu sayede, nicemlenmiş kanal yön bilgisi kullanılarak elde edilebilen toplam güvenlik kapasitesi:

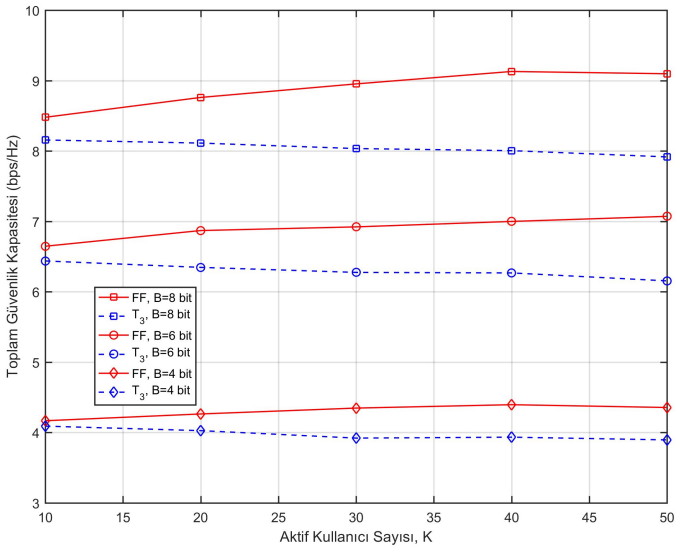
$$R = \sum_{m=1}^{M} \mathbb{E}\left\{\log_2\left(1+\hat{SINR}_{b_m}\right)\right\} - \mathbb{E}\left\{\log_2\left(1+\hat{SINR}_{e_m}\right)\right\}. \tag{78}$$

şeklinde yazılır.

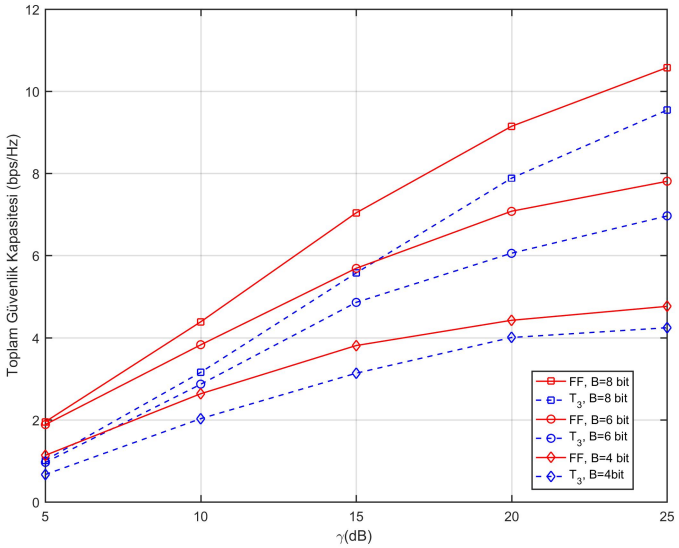
Hüzmeleme vektörü $\hat{\mathbf{W}}$'nın sütunları, nicemlenmiş kanal yön bilgileri kullanılarak oluşturulduğundan mükemmel bir şekilde dik değildir. Bu durum, kullanıcıların sinyalleri arasında karışıma (inter-user interference) yol açmaktadır. Kullanıcıların sinyalleri arasındaki bu karışma, onların algılarını bozmakta ve güvenlik kapasitesini negatif yönde etkilemektedir. Öte yandan, bu karışım gizli dinleyicinin de algısını bozmakta ve onun da kapasitesini düşürmektedir. Nicemleme hatasından kaynaklanan karışım, bu çalışmada önerilen yarı-dik kullanıcı seçimi kriteri ve döndürülmüş kod kitapçığı kullanarak düşürülmektedir. Kullanıcılar arasındaki karışımın tamamen yok edilememesinden dolayı, gizli dinleyicinin algısı bozulmaya devam etmektedir.

Benzetim çalışmaları Bu bölümde, benzetim çalışmaları $N_t = 2$ antenli bir verici için gerçekleştirilmiştir. $\mathcal{T}_3$ kriteri için eşik değeri çifti (γ_{th}, ϵ) her bir hücrede ortalama $\bar{K} = 4$ kullanıcı için hesaplanmıştır: (γ_{th}, ϵ) $[(1.65, 0.4), (2, 0.25), (2.3, 0.2), (2.55, 0.18), (2.6, 0.15)]$ olarak seçilmiştir. Sadece bu eşik değeri çiftini sağlayan kullanıcılar kod kitapçığının belli bir indeksine karşılık gelen nicemlenmiş CDI'larını B bit ile vericiye iletmektedir. Alice geri besleme bilgilerini kullanarak M kullancıyı seçmekte ve ZFBF ile kullanıcılar arasındaki karşımı düşürecek hüzmeleme vektörleri oluşturmaktadır. Bu çalışmada, en kötü senaryo göz önünde bulundurulmuş ve vericinin gizli dinleyici hakkında hiç bir bilgiye sahip olmadığı durum göz önünde bulundurulmuştur.

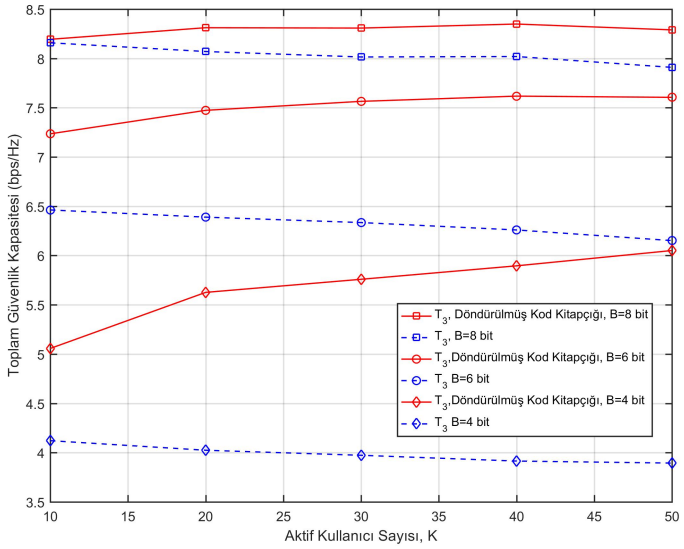
$\mathcal{T}_3$ kriteri ve tam geri besleme yöntemi arasında güvenlik kapasitesi toplamı karşılaştırmaları yapılmıştır. Tam geri besleme yönteminde bir eşik değeri uygulanmaksızın bütün kullanıcılar CDI'larını vericiye yollamaktadır. Bu karşılaştırmalar Şekil 20 ve Şekil 21'de farklı SNR ve aktif kullanıcı sayılarına (K) bağlı olarak verilmiştir. Geri besleme yükü $\%60$ ile $\%92$ arasında düşürülürken, güvenlik kapasitesileri arasındaki fark 0.1bps/Hz-1bps/Hz arasında değişmektedir. Gözlemlendiği üzere, nicemleme bit sayısı B arttıkça tam geri besleme ve $\mathcal{T}_3$ kriteri arasındaki güvenlik kapasitesi farkı artmaktadır. Şekil 22 ve Şekil 23'de döndürülmüş kod kitapçığının $\mathcal{T}_3$ algoritmasına olan etkisi gösterilmiştir.



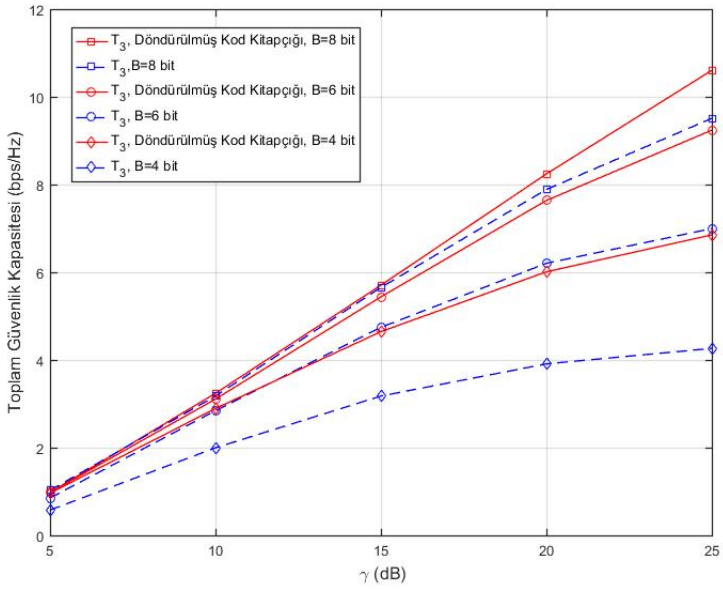
Şekil 20: Güvenlik kapasitesinin tam geri besleme kanalı (FF) ve $\mathcal{T}_3$ kriteri için karşılaştırılması, $\gamma = 20$dB.



Şekil 21: Güvenlik kapasitesinin tam geri besleme kanalı (FF) ve $\mathcal{T}_3$ kriteri için farklı SNR'larda karşılaştırılması.



Şekil 22: $\mathcal{T}_3$ algoritmasının döndürülmüş kod kitapçığı etkisi,$\gamma = 20$dB.



Şekil 23: Farklı SNR'lar için $\mathcal{T}_3$ algoritmasının döndürülmüş kod kitapçığı etkisi.

4.5 Güvenli çoklu kullanıcılı MIMO sistemi

Bu bölümde, çoklu antenli çoklu kullanıcılı bir sistem modeli göz önünde bulundurulmuştur. Çoklu antene sahip verici ($N_t \geq 2$), tek antenli ($N_r = 1$) K sayıdaki aktif kullanıcı arasından, M kullanıcıyı güvenli haberleşme için seçmektedir. Çoklu antene sahip gizli dinleyici ($N_e \geq 2$) ise M kullanıcıya gelen mesaj sinyallerini pasif olarak dinlemektedir. Burada alıcı tarafında kanalların mükemmel bir şekilde kestirildiği fakat verici tarafında kullanıcıların sadece nicemlenmiş kanal bilgilerinin mevcut olduğu varsayılmaktadır. Ayrıca, verici gizli dinleyicinin kanalına dair bir bilgiye sahip değildir. Bundan dolayı, kullanıcılara yollanan bilgi sinyallerini maskelemek için yapay gürültü kullanmaktadır.

Böylece, verici tarafından yapay gürültü ile maskelenerek iletilen mesaj sinyali,

$$\mathbf{x} = \mathbf{W}\mathbf{s} + \mathbf{Q}\mathbf{a}, \tag{79}$$

formundadır. Bilgi sinyali vektörü, $\mathbf{s} = [s_1, s_2, \ldots, s_M]$ olarak gösterilmiştir ve gücü $E\{|s_m|^2\} \leq P_s$'dir. Hüzmeleme vektörü $\mathbf{W} = [\mathbf{w}_1, \mathbf{w}_2 \ldots, \mathbf{w}_m, \ldots, \mathbf{w}_M]$'dir ve ZFBF yöntemi ile $\mathbf{W} = \mathbf{H}(\mathbb{M})^H(\mathbf{H}(\mathbb{M})\mathbf{H}(\mathbb{M})^H)^{-1}$ şeklinde oluşturulmuştur. Burada $\mathbf{H}(\mathbb{M}) \in \mathcal{C}^{M\times N_t}$ kanal matrisine karşılık gelmektedir. Vericideki seçilmiş M kullanıcının kanal vektörleri $\mathbf{h}_m \in \mathcal{C}^{N_t\times 1}$ olarak oluşturulmuştur $\mathbf{H}(\mathbb{M}) = [\mathbf{h}_1, \mathbf{h}_2 \ldots, \mathbf{h}_m, \ldots, \mathbf{h}_M]^T$. Yapay gürültünün hüzmeleyici vektörü $\mathbf{Q}$ ise $\mathbf{H}(\mathbb{M})$ boş uzayının birim dik tabanlarıdır. Yapay gürültü vektörü $\mathbf{a}$ ile gösterilmiştir ve gücü P_a'dır. Toplam güç P, bilgi sinyali ve yapay gürültü sinyallerinin güçlerinin toplamına eşittir ($P_s + P_a$). Bilgi sinyalinin gücü $P_s = \frac{\alpha P}{M}$ ve yapay gürültü sinyalin gücü $P_a = \frac{(1-\alpha)P}{N_t - M}$'dir. α sinyaller arasındaki güç dağılımını ayarlayan parametredir ve değeri $(0, 1)$ aralığındadır.

Yapay gürültü hüzmeleme vektörü $\mathbf{Q}$'nin varlığını garantilemek için N_t'nin M'den büyük olması ve gizli dinleyinin yapay gürültü sinyallerini yok etmesini engellemek için $(N_t - M) \geq N_e$ olması gerekmektedir.

Bu çalışmada, M kullanıcı vericide yarı-dik kriterine dayalı kullanıcı seçimi ile seçilmiştir ve $m.$ kullanıcının aldığı sinyal

$$y_m = \mathbf{h}_m^H \mathbf{w}_m s_m + \sum_{j=1, j\neq m}^{M} \mathbf{h}_m^H \mathbf{w}_j s_j + \mathbf{h}_m^H \mathbf{Q}\mathbf{z} + n_m. \tag{80}$$

olarak yazılabilir.

En kötü senaryo göz önünde bulundurularak gizli dinleyicinin diğer kullanıcılardan gelen girişim sinyallerini yok edebildiği varsayılmıştır. Böylece, $m.$ kullanıcının mesaj sinyali gizli dinleyicide

$$\mathbf{y}_{e_m} = \mathbf{H}^e \mathbf{w}_m s_m + \mathbf{H}^e \mathbf{Q}\mathbf{a} + \mathbf{n}_{e_m}, \tag{81}$$

olarak alınmaktadır. Gizli dinleyicinin kanal matrisi $\mathbf{H}^e \in \mathcal{C}^{N_e\times N_t}$'dir. Kullanıcıların ve gizli dinleyicilerin, karmaşık toplanır beyaz Gauss gürültüleri n_m ve $\mathbf{n}_{e_m}$'nın her elemanı ile gösterilmiştir. Bu gürültüler sıfır ortalamalıdır ve sırasıyla σ^2 ve σ_e^2 varyanslara sahiptir.

Böylece, elde edilebilecek olan güvenlik kapasitesi

$$R = \sum_{m=1}^{M} \left\{ \log_2(1 + SINR_m) - \log_2(1 + SINR_{e_m}) \right\}^+, \tag{82}$$

olarak ifade edilebilir. $SINR_m$ ve SNR_{e_m} sırasıyla kullanıcıdaki ve gizli dinleyicideki $m.$ veri için ani sinyal-gürültü-girişim (SINR) ve ani SNR değerlerini göstermektedir ve sırasıyla aşağıdaki şekilde tanımlanır:

$$SINR_m = \frac{|\mathbf{h}_m^H \mathbf{w}_m|^2}{\sum_{j=1, j\neq m}^{M} |\mathbf{h}_m^H \mathbf{w}_j|^2 + \frac{1-\alpha}{\alpha} \frac{M}{N_t - M} |\mathbf{h}_m^H \mathbf{Q}|^2 + \frac{1}{\gamma}}. \tag{83}$$

Burada γ Bob'un ortalama SNR değeridir.

$$SINR_{e_m} = (\mathbf{H}^e \mathbf{w}_m)^H \left(\frac{1-\alpha}{\alpha} \frac{M}{N_t - M} (\mathbf{H}^e \mathbf{Q})(\mathbf{H}^e \mathbf{Q})^H \right)^{-1} (\mathbf{H}^e \mathbf{w}_m). \tag{84}$$

Alice'de Eve'in CSI ile ilgili herhangi bir olmadığı varsayıldığından σ_e sıfır olarak kabul edilmiştir.

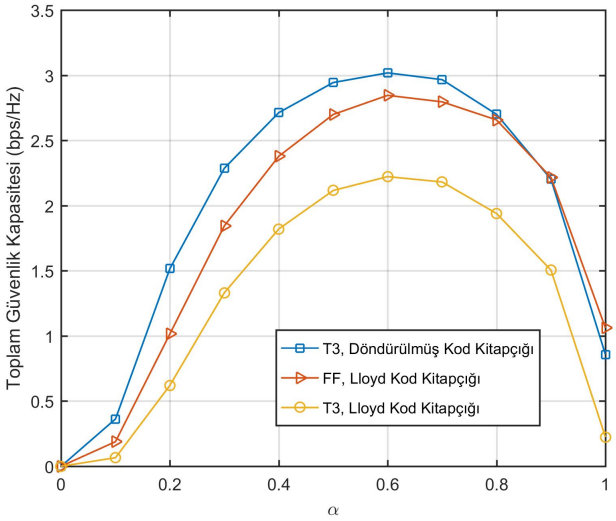
Benzetim sonuçları Bu bölümde, çoklu kullanıcılı MIMO (MISOME) sistemler için yapılan benzetim çalışmalarının sonuçları sunulmaktadır. Vericideki anten sayısı $N_t = 4$ alınmıştır. İki kullanıcı güvenli haberleşme için seçilmiş olur ($M = 2$) gizli dinleyicideki anten sayısı $N_e = 2$'dir. $\bar{K} = 4$ olması için kullanıcı sayıları $K = [10, 20, 30, 40, 50]$ ve onlara uygun olan eşik değerleri $\gamma_{th} = [0.6, 0.6, 0.6, 0.6, 0.6]$ ve $\epsilon_{th} = [0.465, 0.370, 0.322, 0.293, 0.272]$ olarak hesaplanmıştır. Bu eşik değerlerine göre $\mathcal{U}_2$ kümesi elde edilmiş, ve seçilen yetkili kullanıcıların CDI bilgileri Lloyd tabanlı ve döndürülmüş kod kitapçığı'na göre B bit kullanılarak Alice'e iletilmiştir.

Şekil 24'de farklı geri besleme modelleri ve kod kitapçığı tasarımı için toplam güvenlik kapasitesinin değişimi gösterilmiş olup $\mathcal{T}_3$ kriteri algoritması ve döndürülmüş kod kitapçığı kullanıldığında toplam güvenlik kapasitesinin maksimum olduğu değer 0.5 olarak belirlenmiştir.

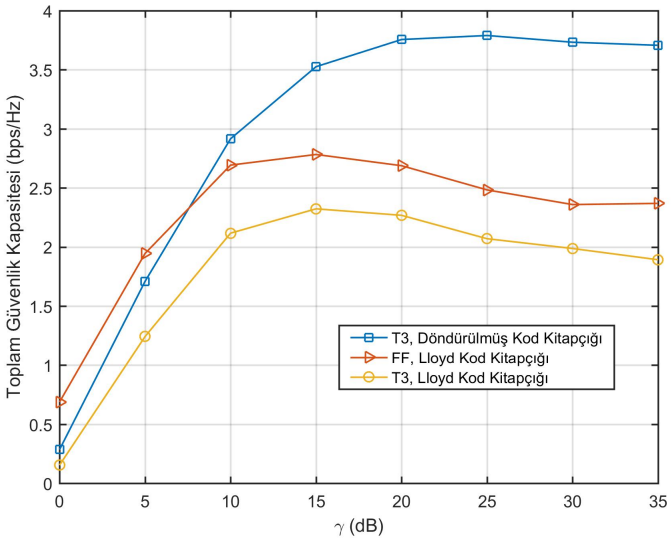
Şekil 25'de farklı geri besleme modelleri ve ortalama SNR değerleri için toplam güvenlik kapasitesi gösterilmiş olup geri besleme kanal yükü azaltıralarak döndürülmüş kod kitapçığı ve $\mathcal{T}_3$ kriteri algoritmasının toplam güvenlik kapasitesini arttırıldığı gözlemlenmiştir.

Şekil 26'de farklı geri besleme modelleri ve aktif kullanıcı sayısına göre toplam güvenlik kapasitesi gösterilmiş olup geri besleme kanal yükü azaltıralarak döndürülmüş kod kitapçığı ve $\mathcal{T}_3$ kriteri algoritmasının toplam güvenlik kapasitesini arttırıldığı gözlemlenmiştir. Aktif kullanıcı sayısı arttığında güvenlik kapasitesinin çoklu kullanıcı çeşitleme tekniğinden dolayı daha da artış gösterdiği gözlemlenmiştir.

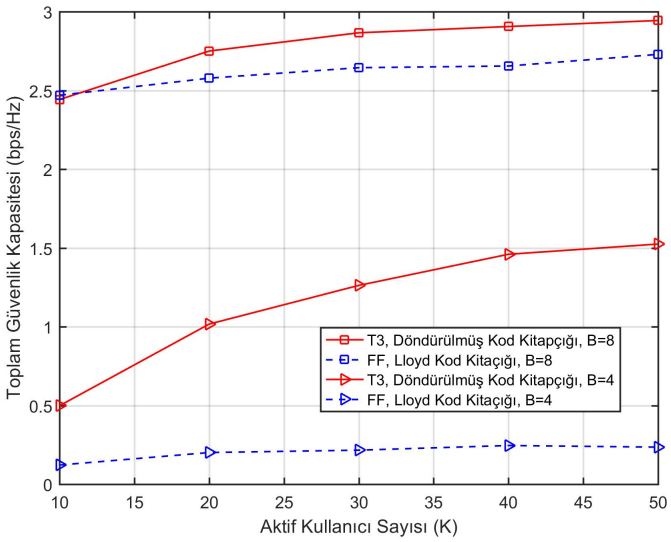
Şekil 27'de bir ve birden fazla Bob seçiminin etkisi tekli ve çoklu kullanıcı güvenlik kapasitesi gösterilmiş olup birden fazla yetkili kullanıcıya hizmet verildiğinde güvenlik kapasitesinin arttığı gözlemlenmiştir.



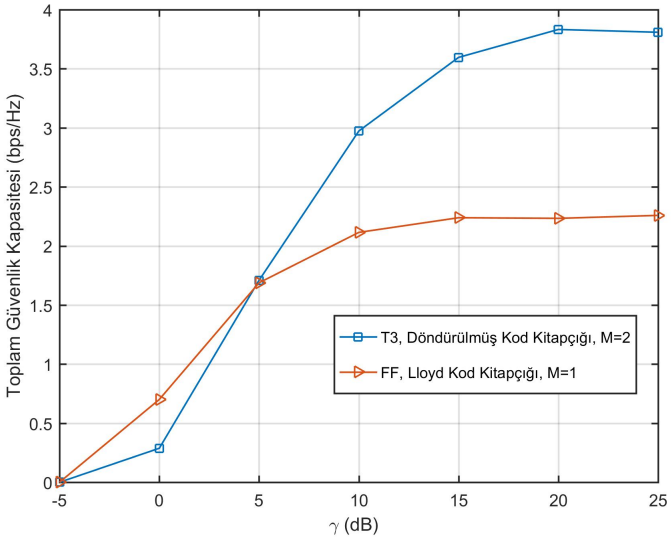
Şekil 24: Toplam güvenlik kapasitenin α'ya göre değişimi, $\gamma = 10dB$, $K = 50$, $M = 2$, ve $B = 8$



Şekil 25: Toplam güvenlik kapasitenin α'ya göre değişimi, $\alpha = 0.5$, $K = 50$, $M = 2$, ve $B = 8$



Şekil 26: Toplam güvenlik kapasitesinin K'ya göre değişimi, $\alpha = 0.5$, $\gamma = 10dB$, $M = 2$, ve $B = 8$.



Şekil 27: Farklı M için γ'ya karşılık güvenlik kapasitesi, $\alpha = 0.5$, $K = 50$, ve $B = 8$.

4.6 Pre-FFT hüzmeleme uygulaması

MIMO sistem ile OFDM kombinasyonu yeni nesil haberleşme sistemleri için etkili çözümler üretmektedir. Çoklu anten kullanımıyla birlikte, hüzmeleme (beamforming) uygulamaları hayati bir önem taşımaktadır. Hüzmeleme teknikleri, haberleşmenin karakteristiklerine uygun biçimde uygulanmıştır. Hüzmeleme metodlarından pre-FFT (Fast Fourier Transform) seçilerek, alıcı ve verici tarafta uygulanarak, MIMO-OFDM sistem için noktadan noktaya iletişim yazılım tabanlı radyolar üzerinde gerçeklenmiştir [117]. Gerçekleme için NI USRP 2921 yazılım tabanlı radyo modeli ve LabVIEW yazılımı kullanılmıştır. Sistem performans kalitesi, farklı hüzmeleme katsayılarına göre hata vektör büyüklüğü (Error Vector Magnitude, EVM) ve bit hata oranı (Bit Error Rate, BER) elde edilerek gözlemlenmiştir.

Çalışma [124]'da, uyarlanabilir aralıklı hüzmeleme ile simülasyon sonucu göstermiştir ki, MIMO-OFDM sistemde hüzmeleme uygulaması sistem kapasitesini ve bant genişliği verimliliğini geliştirmiştir. [125] çalışmasında dikgen hüzmeleme tekniğiyle MIMO-OFDM sistem performansının yükseldiğini incelemiştir. Simülasyon sonuçları dikgen hüzmeleme tekniğinin uygulandığı MIMO-OFDM sisteminin SINR değerinin geleneksel MIMO-OFDM sisteme göre daha yüksek olduğunu göstermiştir. [126] çalışmasında OFDM haberleşme sisteminde pre-FFT hüzmeleme uygulaması benzetim çalışmaları yapılmıştır. Ayrıca sinyaller arası açısal ayrışma gözlemlenmiştir. Sayısal sonuçlara göre, hüzmeleme tekniğinin performansı iyileşmesini sağladığı görülmüştür. [127] çalışmasında hüzmeleme kullanılan akıllı anten ağlarına odaklanılmıştır. Test sonuçlarıyla birlikte, sayısal ve analog hüzmelemenin avantajları vurgulanmıştır. [128] çalışmasında, GNU-radyo kullanılarak dağıtık hüzmeleme incelenmiştir. [129] çalışmasında sanal anten tekniği kullanılarak uygulanan hüzme şekillendirmenin üstünde durmuştur. [130] çalışmasında, hüzmeleme için pre-FFT ve post-FFT adaptif dizileri kullanılarak OFDM sistemde simülasyon sonuçları gözlenmiştir. Sonuçlar pre-FFT için dizi işlemenin çok yollu durumlar için daha az sayıda olduğunu göstermiştir.

Çalışma [131]'te, kablosuz yerel alan ağı (local area network, LAN) için pre-FFT ve post-FFT hüzmeleme metodlarının simülasyon sonuçlarını karşılaştırmıştır. Sonuçlar incelendiğinde, pre-FFT hüzmelemenin basitlik ve maliyet açısından daha iyi olduğu görülmüştür. Çalışma [132], OFDM tabanlı sistemlerde en küçük ortalama kareler (Least Mean Square, LMS) hüzmeleme methodu ile pre-FFT ve post-FFT birleşimi sayesinde, girişim yok edilmiştir ve pre-FFT daha az karmaşık olması sebebiyle post-FFT'ye göre daha tercih edilebilir olduğu vurgulanmıştır. [133] çalışmasına göre, pre-FFT hüzmeleme, geleneksel hüzmeleme uygulamalarına göre sistem yapısında önemli maddi azalımlar sağlamaktadır. [134] çalışmasında, pre-FFT kullanılan akıllı anten algoritmalarının kanal kestirimine etkisi üzerinde durulmuştur. Bazı senaryolardaki simulasyon sonuçları, 2 ayrı pre-FFT algoritması kullanılarak sönümlenmiş çoklu-yola karşı OFDM sistem dayanıklılığının gelişimini göstermektedir. [135] çalışmasında, LMS algoritması ve pre-FFT tabanlı farklı senaryoları simule edilmiştir. Simulasyon sonuçlarında, adaptif hüzmeleme senaryolarının daha iyi ortalama karesel hata (Mean Square Error, MSE) performansına sahip olduğu görülmektedir. [136] çalışmasında ise OFDM sistemleri için hüzme uzayı tabanlı pre-FFT hüzmeleme algoritması incelenmiştir. Yapılan simulasyonlara göre pre-FFT hüzmeleme algoritması, geleneksel adaptif hüzmeleme algoritmasıyla kıyaslandığında, daha iyi bir BER

performansına sahip olduğu görülmektedir.

Çalışma [137], OFDM sistemler için özyinelemeli en küçük kareler (Recursive Least Square, RLS) tabanlı pre-FFT adaptif hüzmeleme incelemiştir. Karmaşıklığı azaltmasıyla, iyi yakınsama performansı göstermektedir. Referans sinyal kullanılarak kanal durumunun takip edilmesiyle, düşük sayısal karmaşıklık ve güçlü BER performansı elde edilmektedir. Önerilen çalışma, alıcı ve verici tarafında pre-FFT hüzmeleme metodu kullanılarak oluşturulan noktadan noktaya MIMO-OFDM sisteminin gerçek zamanlı SDR uygulamasında ilk olmaktadır.

4.6.1 MIMO-OFDM ve hüzmeleme

MIMO-OFDM sistemi için n. alttaşıyıcı için frekans ortamında MIMO kanalın modeli 85'de verilmiştir.

$$\mathbf{y}(\mathbf{n}) = \mathbf{H}(\mathbf{n}) * \mathbf{x}(\mathbf{n}) + \mathbf{n}(\mathbf{n}) \tag{85}$$

Burada $\mathbf{y}(\mathbf{n})$, alınan OFDM sinyalinin sütun vektörü, $\mathbf{H}(\mathbf{n})$ çokyollu kanal matrisi, $\mathbf{x}(\mathbf{n})$ ise iletilen OFDM sinyalinin sütun vektörü ve $\mathbf{n}(\mathbf{n})$ ise AWGN'nin sütun vektörüdür

Uzamsal çoğullama tekniğinin bir uygulaması olarak MIMO, OFDM çıktısının iki anten tarafından iletilmesiyle gerçekleştirilir. Aynı zamanda alıcı kısımda da alım işlemi için iki anten kullanılır. Bunun sonucunda sistemde dört farklı kanal bileşeni mevcuttur. 2x2 MIMO için hüzmeleme işlemi Şekil 28'da görülmektedir.

MIMO-OFDM sisteminde $h_{11}(n)$, $h_{12}(n)$, $h_{21}(n)$ ve $h_{22}(n)$ 4 farklı MIMO kanal bileşenlerini içeren $\mathbf{H}(n)$ kanal matrisini oluşturur.

$$\begin{bmatrix} y_1(n) \\ y_2(n) \end{bmatrix} = \begin{bmatrix} h_{11}(n) & h_{12}(n) \\ h_{21}(n) & h_{22}(n) \end{bmatrix} * \begin{bmatrix} x_1(n) \\ x_2(n) \end{bmatrix} + \begin{bmatrix} n_1 \\ n_2 \end{bmatrix} \tag{86}$$

Sistemde, gerçek zamanlı gerçeklenmesinin kolaylığı yüzünden pre-FFT hüzmeleme tekniği seçilmiştir. Verici tarafta, iletilecek OFDM modülatör çıktıları iki hüzmeleme katsayısı ile çarpılır ve toplanır.

$$S_t(n) = \alpha_1 x_1(n) + \alpha_2 x_2(n) \tag{87}$$

Burada $x_1(n)$ ve $x_2(n)$, iki kaynak düğüm antenlerinden iletilen OFDM sembollerini temsil etmektedir. α_1 ve α_2 ise verici için hüzmeleme katsayılarıdır. Bu katsayılar hüzmenin 0 veya 90 derecedeki konumuna göre belirlenmiştir. Alıcı tarafta ise iki alıcı antene gelen işaretler aşağıdaki formülasyonlarda sırayla gösterilmiştir.

$$y_1(n) = \alpha_1 x_1(n) * h_{11}(n) + \alpha_2 x_2(n) * h_{12}(n) \tag{88}$$

$$y_2(n) = \alpha_1 x_1(n) * h_{21}(n) + \alpha_2 x_2(n) * h_{22}(n) \tag{89}$$

$y_1(n)$ ve $y_2(n)$, iki alıcı düğüm antenleri tarafından alınan zaman ortamında hüzmelenmiş OFDM sembollerini temsil etmektedir. Ardından alınan bu semboller alıcı için β_1 ve β_2

hüzmeleme katsayıları ile çarpılarak $s_r(n)$ elde edilir ve bu hüzmeleme işlemleri sonucunda oluşan zaman ortamındaki işaret aşağıdaki gibi elde edilir:

$$s_r(n) = \beta_1 \cdot y_1(n) + \beta_2 \cdot y_2(n) \tag{90}$$

4.6.2 Test Düzeni

Donanım ve Yazılım Bileşenleri Noktadan noktaya MIMO-OFDM sistemde pre-FFT hüzmeleme tekniği gerçeklemesi, İTÜ Telsiz Haberleşme Araştırma Laboratuvarı'nda (THAL) yapılmıştır. Sistem programı, LabVIEW yazılımının temel elemanlarından olan sanal cihazlar kullanılarak oluşturulmuştur. Verici ve alıcı için ikişer NI USRP 2921 birimi kullanılmıştır.

Veri İşleme Yöntemi Test sisteminin verici kısmında; LabVIEW'deki USRP kütüphanesinden oturum başlatma, parametre konfigürasyonları ve iletilen işaretin özelliklerini belirlemek için ilgili sanal enstrümanlar (virtual instrument, VI) kullanılmıştır. Data SubVI içerisinde OFDM çerçeve yapısı ayarlamaları yapılmıştır. Sayısal modülasyon kütüphanesinden seçilen sözde gürültü (pseudo noise, PN) kullanılarak MT Generate Bits VI ile verici tarafından gönderilen bitler üretilmiştir. Referans semboller ise verici tarafından bilinerek sabit olarak belirlenmiştir. Testlerde modülasyon çeşidi olarak dört bölmeli faz kaydırmalı anahtarlama (quadrature phase shift keying, QPSK) seçilerek, iletilen bitler sembollere çevrilmiştir. Dizi (array) VI'ları kullanılarak çerçeve yapısı sağlanmış, alt-taşıyıcı atamaları yapılmıştır. Bilgi sembolleri ve referans semboller bu sayede her 8 bilgi sembolü için 1 referans sembolü olacak şekilde kolayca dizme işlemi uygulanmıştır. Ardından sıfır ekleme (zero padding, ZP) işlemi ile 0 alt-taşıyıcıları yerleştirme bloğu da uygulanmıştır.

Toplamda 40 adet referans sembolü kullanılmış ve 320 bilgi sembolü ile toplam 360 sembol ortadan ikiye bölünerek sıfır ekleme uygulanmıştır. 60 ZP çerçevenin başına, 1 tane DC bileşeninde, 59 tane çerçeve sonunda bulunmaktadır. Seri-paralel dönüşümünün ardından ters ayrık Fourier dönüşümü (Inverse Fast Fourier Transform, IFFT) için LabVIEW kütüphanesinden IFFT VI ile uygulanmıştır. Ön ek (Cyclic Prefix, CP) ekleme dizi VI ile çerçevenin yüzde 25'i kopyalanarak başlangıca eklenmiştir. Verici bloğu, çıktılar α_1 ve α_2 ile çarpılıp toplandıktan sonra iletim ve oturumun kapatılmasından sorumlu USRP VI'ları kullanılarak tamamlanmıştır. Sistem parametreleri Çizelge 2'de gösterilmiştir.

Alıcı bloğunda, NI PXI donanımının vektör işaret analizör kartı (vector signal analyzer, VSA) daha iyi donanımsal özellikler nedeniyle tercih edilmiştir. Alıcı kısmında, LabVIEW yazılımında USRP kütüphanesi yerine RFSA kütüphanesi kullanılmıştır. Verici kısımdaki ayarlamalara benzer işlemler yapılmıştır. Alınan veri β_1 ve β_2 hüzmeleme katsayıları ile çarpılarak toplanmıştır. Farklı olarak, alınan işaretin frekansta oluşan sapmayı (Carrier Frequency Offset, CFO) engellemek için CFO tahmini yapılan bir blok üretilmiştir. Çerçevedeki ön ek kısım bilgisi kullanılarak algoritmasına dayanarak frekansta oluşan sapmanın en büyük olabilirlik kestirimi (maximum likelihood estimation) ile CFO hesaplanmış ve düzeltilmiştir. Ardından ön ek kısmı kaldırıldı ve FFT bloğu ile ayrık Fourier dönüşümü gerçekleştirilmiştir. ZP kısmı çıkartılmış ve referans semboller bilgi sembollerinden ayrılmıştır. Kanal tahmin ve dengeleyici blokları ile

Çizelge 2: Sistem Parametreleri

Taşıyıcı Frekans	2.45 GHz
İletim Kazancı	10 dB
Alıcı Kazancı	10 dB
I/Q Veri Oranı	1 MS/sec
Bir Çerçevedeki Bit Sayısı	640
Referans Alttaşıyıcı Sayısı	320
Referans Alttaşıyıcı Sayısı	40
Zero Padding Uzunluğu	120
FFT Uzunluğu	480
Ön Ek Uzunluğu	120
Çerçevedeki Toplam Alt Taşıyıcı Sayısı	600

kanal etkileri en aza indirilmiş ve bilgi verileri elde edilmiştir. Ardından bit hata oranı (BER) ve hata vektör büyüklüğü (error vector magnitude, EVM) hesaplama işlemleri yapılmıştır.

4.6.3 Sonuçlar

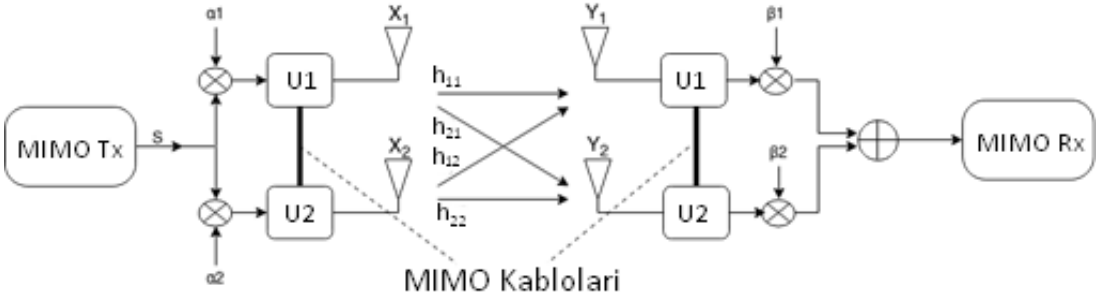
Test kurulum bölümünde açıklanan pre-FFT hüzmeleme kullanılan noktadan noktaya MIMO-OFDM sistem performansı, değişik konfigürasyonlardaki testlerle gözlenmiştir. Performans değerlendirmeleri için, LabVIEW kodundaki bazı parametreler değiştirilmiştir. Her kaynak bilgisi QPSK modülasyon tekniği kullanılarak iletilmiştir. Alınan hüzmelenmiş bilgilerle, BER ve EVM değerleri hesaplanmıştır.

EVM değerleri, modülasyonun kalitesi ve kablosuz haberleşme sistemleri için hata performansının bir ölçüsüdür. EVM, gürültü gibi bütün potansiyel faz ve genlik bozunumlarının ölçülmesinde ürün veya bir devrenin kalitesi hakkında kapsamlı bir değerlendirme yapılabilmesinde önemli rol oynar. Bozuklukların varlığında demodülatör performans ölçümü olan hata vektör büyüklüğü, IQ düzlemindeki fazörleri kullanarak ideal sembol vektörü ile gerçek ölçüm vektörünün boyut ve konum farklılığını karşılaştırmaktadır. Şekil 30'de gösterildiği gibi bu vektörler arasındaki farklılık EVM'i verir. I_j alınan $j.$ sembolün reel bileşenini, Q_j ise sanal bileşeni göstermek üzere, EVM değerleri [138]:

$$EVM = \frac{\sqrt{\frac{1}{N}\sum_{k=1}^{N}\left[\left(I_k - \hat{I}_k\right)^2 + \left(Q_k - \hat{Q}_k\right)^2\right]}}{|v_{max}|} \tag{91}$$

olarak hesaplanabilir. 91'da $\hat{I}_j$ ve $\hat{Q}_j$ alınan ideal $j.$ sembolün reel ve sanal bileşenlerini, $|v_{max}|$ ise alınan ideal sembol vektörünün maksimum değerini ifade etmektedir. N toplam gönderilen sembol sayısıdır.

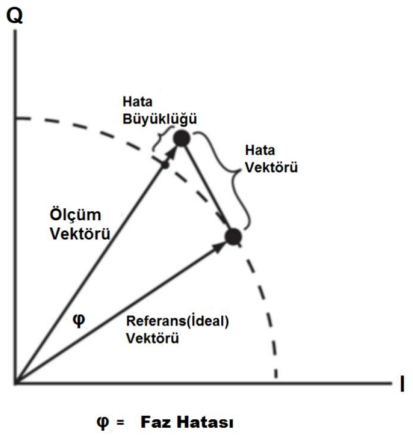
Sistem performansı, hüzmelemenin sistem performansını nasıl geliştirdiğinin gösterilmesi için ölçülmüştür. Bu ölçümler, farklı hüzmeleme katsayı çiftleriyle tekrarlanmıştır. EVM ve BER değerleri, Çizelge 3'de gösterilen katsayı çiftlerinin 16 adet kombinasyonuyla ölçülmüştür. En



Şekil 28: MIMO Hüzmeleme Yapısı

Alt Taşıyıcı Indisi	0-59	60-239	240	241-420	421-479
	ZP Serisi	Bilgi + Referans	DC	Bilgi + Referans	ZP Serisi
Verici	60 Örnek	180 Örnek	0	180 Örnek	59 Örnek
Alıcı	60 Örnek	180 Örnek	0	180 Örnek	59 Örnek

Şekil 29: Çerçeve Yapısı



Şekil 30: EVM: İdeal fazör vektörünün pozisyonu ile alınan fazör vektörü arasındaki fark.

iyi sonuçlar, $\alpha_1 = j$, $\alpha_2 = 1$ iken ortaya çıkmaktadır. Optimum hata performansı ise $\alpha_1 = j$, $\alpha_2 = 1$, $\beta_1 = j$ ve $\beta_2 = 1$ olduğunda oluşmuştur. $\alpha_1 = 1$ ve $\alpha_2 = 1$ olduğunda ise en kötü sistem performansı oluşmuştur. BER değerinin 0 değerinden $1,85 \times 10^{-6}$' ya yükselmesine sebep olan en kötü sistem performansı ise $\alpha_1 = 1$, $\alpha_2 = 1$, $\beta_1 = j$ ve $\beta_2 = 1$ iken gerçekleşmiştir. Hüzmelemenin sistem performansını etkilediği ve performans sonuçlarında büyük değişikliklere sebep olduğu çok açık görülmektedir. Ayrıca, kaynak ve hedef VI lar arasındaki iletim kalitesini göstermek için yıldızkümesi diyagramları oluşturulmuştur.

Çizelge 3: Farklı hüzmeleme katsayıları için EVM ve BER değerleri

α_1	α_2	β_1	β_2	EVM	BER
1	1	1	1	7,305	0
1	1	1	j	8,722	0
1	1	j	1	10,392	$1,85 \times 10^{-6}$
1	1	j	j	8,104	0
1	j	1	1	6,543	0
1	j	1	j	7,117	0
1	j	j	1	6,308	0
1	j	j	j	7,062	0
j	1	1	1	5,987	0
j	1	1	j	6,231	0
j	1	j	1	5,908	0
j	1	j	j	6,286	0
j	j	1	1	9,883	0
j	j	1	j	9,406	0
j	j	j	1	8,366	0
j	j	j	j	9,86	0

4.7 SISO sistemler için fiziksel katman güvenliğinde karşılıklı kanal özelliğine dayalı anahtar üretimi

Bu bölümde A ve B, iki haberleşme düğümü olduğu varsayıldığında, A düğümünden B düğümüne olan kanal için elde edilen kanal katsayıları ile, B düğümünden A düğümüne olan kanal için elde edilen kanal katsayılarının benzerliği incelenmiştir [118] . Karşılıklı kanal özelliğinden dolayı bu kanalların birbirine benzer çıkmaları beklenmektedir. SISO vericide ve alıcıda tek antene sahip bir sistemdir.

Literatürde kanalın karşılıklı olma özelliğinin incelendiği birçok araştırma vardır. Bu çalışmalarda verici ile alıcı arasında karşılıklı kanal olduğu varsayılmıştır. Kanalın bu karşılıklı özelliği sayesinde verici ve alıcı, kanalı fiziksel katman güvenlik anahtar üretimi için ilişkili, verimli bir kaynak olarak görecektir. Bunun sebebi, kaynakların ilişkili olması dışında, kablosuz kanal olması sebebiyle kaynağın herhangi bir yerde bulunabilir olması ve kanalın zamansal ve mekânsal etki ile hızlıca değişmesinden, gizli dinleyiciler için kaynak çözümünün zor olmasıdır. Teorik ve pratik açıdan bu konu [141–143] çalışmalarında incelenmiştir. [144–146] çalışmalarında ise, kanalın zamanda çok kısa bir an için sabit kaldığını ve bu sürede kanalın karşılıklı olma özelliği altında faz farkı kullanılarak anahtar üretme işlemleri incelenmiştir. [147] çalışmasında, kanalın karşılıklı olduğu varsayımı, kimlik doğrulama için kullanılırken kanal durum bilgisine (CSI) dayalı anahtar üretme çalışmaları yapılmıştır. Bu çalışmanın bir diğer önemli özelliği, yazılım tabanlı radyo (SDR) altyapısına sahip USRP ve GNU kullanılarak testler gerçekleştirilmiştir.

[148] çalışmasında ise eş zamanlı çift yönlü zaman bölmeli (TDD) sistemlerde karşılıklı kanal başarısı analiz edilmiş ve ölçüm sonuçları bu başarıyı onaylamıştır. [154] çalışmasında, kanalın karşılıklı olmasının sistem yükünü azaltma yönünde bir avantaja sahip olduğu belirtilmiştir ve böylece daha pratik sistemler tasarlanmasına olanak sağlanmıştır. [149] çalışmasında, TDD-LTE (Uzun Süreli Evrim) sistemlerinde verimli karşılıklı kanal kullanıldığında, kanal durum bilgisi geri bildirim yükü azaltılmış, analiz ve simülasyon sonuçları ise daha iyi bir sistem performansı elde edildiğini göstermiştir. [150] çalışmasında da implante cihazlar için kullanılan elektrik veya manyetik alanların iletimi temelli veri iletişim sistemleri için başlıca problem olabilecek kanal simetrikliği incelenmiş ve sonuçlar göstermiştir ki, sinyal transfer karakteristikleri aynı olduğu ve böylece kanalın karşılıklı özelliğinin geçerli olduğu görülmüştür. [151] çalışmasında ise, kanalın karşılıklı olma durumu değil, 802.11g kablosuz sistemin kanal karakterizasyonu LabVIEW programı ve National Instruments Universal Software Radio Peripheral (NI-USRP) yazılım tabanlı radyoları kullanılarak gerçekleştirilmiştir.

4.7.1 Test Düzeni ve Sonuçları

Laboratuvarda testler için biri verici biri alıcı durumunda olan iki USRP aralarında 70 cm uzaklık olacak şekilde Şekil31 kullanılmıştır. Daha önce anlatılan OFDM sistem modelinin aynısıdır. Yalnızca denkleştirme işlemi uygulanmamış 360 referans sembol gönderimi yapılmıştır.

Testlerde QPSK modülasyon çeşidi seçilmiştir ve sistem parametreleri Çizelge 4'de gösterilmiştir.

360 referans sembolünün 320'si kullanılarak her bir çerçeveden, 1x320 boyutlu kanal kat-

Çizelge 4: Sistem Parametreleri

Taşıyıcı Frekans	2.45 GHz
İletim Kazancı	20 dB
Alıcı Kazancı	30 dB
I/Q Veri Oranı	1 MS/sec
Bir Çerçevedeki Bit Sayısı	640
Referans Alttaşıyıcı Sayısı	360
Zero Padding Uzunluğu	120
FFT Uzunluğu	480
Ön Ek Uzunluğu	120
Çerçevedeki Toplam Alt Taşıyıcı Sayısı	600

sayısı vektörü elde edilmektedir. A USRP biriminden, B USRP birimine toplamda 320000 kanal katsayısı, $i \in \{1, 2, ..., 1000\}$ olmak üzere $h_{AB,i}$ şeklinde kanal katsayısı vektörü elde edilmiştir. B USRP biriminden, A USRP birimine de aynı işlem gerçekleştirilerek $h_{BA,i}$ kanal katsayısı vektörü elde edilmiştir.

Testler sonucunda elde edilen $h_{AB,i}$ ve $h_{BA,i}$ kanal katsayı vektörlerinin ortalaması alınarak elde edilen ortalama kanal vektörlerinin (h_{AB} ve h_{BA}) genlik ve faz bilgileri gözlenmiştir. A USRP biriminden B USRP birimine olan kanal AB, B USRP biriminden A USRP birimine olan kanal BA şeklinde gösterilmek üzere Şekil 32a ve Şekil 32b'de kanal katsayısı vektörleri için genlik ve faz ortalama değerleri gösterilmiştir.

4.8 MIMO sistemler için fiziksel katman güvenliğinde karşılıklı kanal özelliğine dayalı anahtar üretimi

2x2 MIMO sistemde OFDM tekniği kullanılarak sistemde karşılıklı kanal durumunun varlığı incelenmiştir. Karşılıklı kanal çiftlerinin bu incelemeye göre ilişkisi incelerek ilinti katsayıları bulunmuştur. Nicemleme işlemi ile anahtar üretimi yapılmıştır. Sistem modeli olarak daha önce MIMO bölümünde anlatılan model kullanılmıştır. SISO için geçerli olan denkleştirme bloğunun kullanılmaması durumu burada da geçerlidir. MIMO sistem için karşılıklı kanal özellik modeli Şekil 33'deki gibidir.

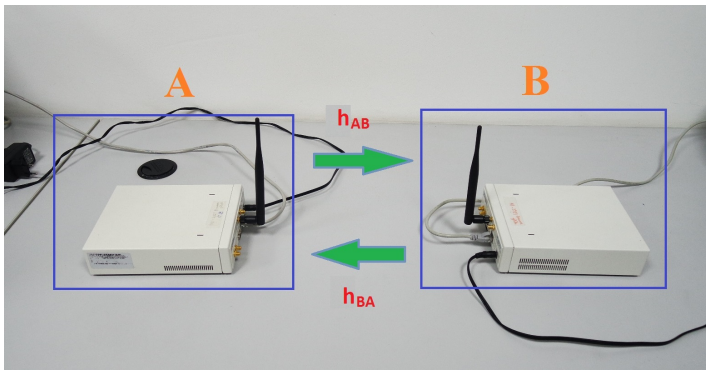
[152] çalışmasında, yukarı ve aşağı bağlantı radyo kanallarının uzaysal karşılılık durumu frekans bölmeli çoğullama (Frequency division duplexing, FDD) sistem için W-CDMA yukarı ve aşağı yönlü bağlantı taşıyıcıları yüksek oranda ilişkili bulunmuştur. [153] çalışmasında ise 4x4 çoklu giriş çoklu çıkış (MIMO) sistemleri için performans kapasitesi gözlenmiştir. Ters eş zamanlı çift yönlü frekans bölmeli (FDD) sistem kanalından, karşılıklı kanal yaklaşımı ile elde edilen kanal durum bilgisi ile sistemin performansında iyileşmeler olduğu görülmüştür.

Çalışma [155]'da, gerçek zamanlı kablosuz araştırmalar için donanım platformu olarak bilinen WARP kullanılarak, OFDM-TDD (Time Division Duplexing, Zaman Bölmeli Çoğullama) sistemde, aşağı ve yukarı yönlü kanal kestirimleri gözlemlenmiş ve sonuçlar göstermiştir ki, aşağı ve yukarı yönlü kanal genlik değerleri karşılıklıdır. RF ön yüz kusurlarından ötürü faz değerleri ise sapmalara uğrar. Çalışma [156], MIMO sistemde TDD tekniği ile karşılıklı kanal durumu incelenmiş ve RF bileşenlerindeki idealsizliklerine rağmen, bu küçük hatalar gözardı edilerek, pratik kullanım için kabul edilebilir olduğu görülmüştür.

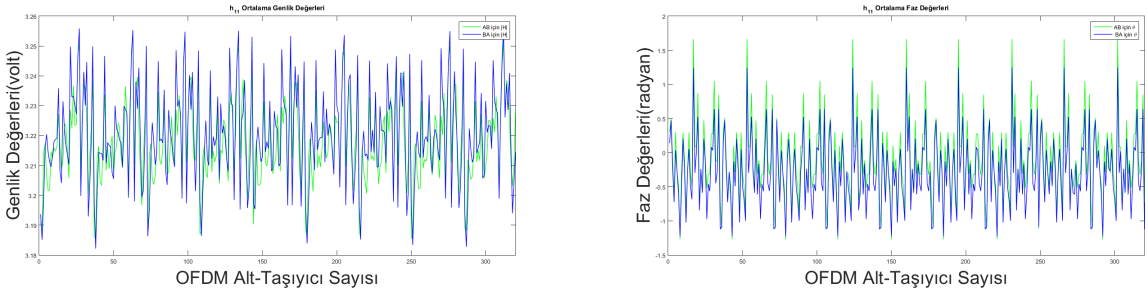
[157] çalışmasında bazı ideal olmayan durumlar ve RF önyüz eksikliklerinin etkisi olsa bile, kanalın karşılıklı olma durumu MIMO sisteme uygulanmış ve sonuçlar karşılıklı kanalın verimliliğini ispat etmiştir. [158, 159] çalışmalarında ise, MIMO tabanlı sistemde karşılıklı kanal varsayımı ve RF önyüz eksikliği etkisi aynı şekilde incelenmiştir. Sonuç olarak, RF önyüz kusurlarının, karşılıklı kanal varsayımını olumsuz yönde etkileyebildiği gözlemlenmiştir. [160] çalışmasında da, TDD-MIMO sistemde IQ dengesizliğinin karşılıklı kanal durumuna etkisi incelenmiş ve çeşitli algoritmalar ile bu dengesizlik telafi edilmeye çalışılmıştır.

Çalışma [161], adaptif 4x4 MIMO sistemde karşıt FDD kanaldan karşılıklı kanal özelliği ile elde edilen kanal durum bilgisi ile sistem kapasitesinin arttığı ve performansın iyileştiği görülmüştür. [162] çalışmasında ise çeşitli MIMO iletim senaryolarında karşılıklık kanal durumu gerçeklenmiş ve gözlemlenmiştir. Karşılıklı kanal durumu ortalama spektral verimi $\%40$, veri hacminde ise $\%20$ oranında kazanç sağlamıştır. Geri besleme yükü, karşılıklı kanal özelliği kullanılarak azaltılmıştır. [163] çalışması karşılıklı kanal durumunun sistem fazla yükünü azaltma gibi avantajlara sahip olduğunu ve böylece pratik sistem dizayn edilebileceğini gözlemlemiştir. Çalışma [164], TDD-LTE için karşılıklı kanal durumunu gerçeklemiş ve geri besleme yükünü azaltarak daha iyi bir sistem performansı elde etmiştir. [168], [169] çalışmalarında vericide CSI için pratik olarak MIMO-TDD sistemde kanalın karşılıklı durumu gerçeklenmiş, sistem kapasitesinin artarak, teorik limitlere yaklaştığı gözlemlenmiştir.

[170], ultra geniş band (ultra wideband, UWB) haberleşmede karşılıklı kanal durumu için deneyler yapılmış, sonuçlar kanalın yüksek oranda karşılıklı olduğunu göstermiştir. İleri ve

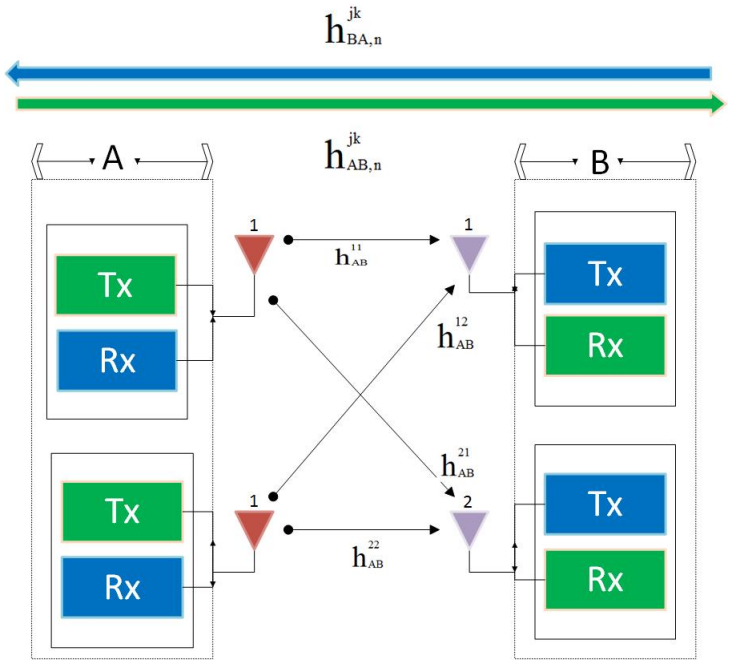


Şekil 31: SISO için Ölçüm Düzeneği



(a) $|h_{11}|$ (b) $\angle h_{11}$

Şekil 32: SISO sistemde 2 kanalın genlik ve faz değerleri



Şekil 33: MIMO Sistem için Karşılıklı Kanal Özellik Modeli

geri yönlü linklerde elde edilen dalga formlarının birbirine özdeş olduğu ve aralarındaki ilinti katsayısının 0.98 gibi yüksek bir değer olduğu görülmüştür. [171], [172], [173] çalışmalarında, MIMO kanallarının ilişkileri bina içi senaryolarda analiz edilmiştir. Farklı MIMO kanallarının birbirleriyle ilişkileri incelense de, ilinti katsayıları ölçülen sinyalin genlik ve faz bilgileri göz önüne alınarak bulunmuştur.

Çalışma [174] tersinir kanalların ilişkisi incelenmese de, her alt-taşıyıcı başına ilinti katsayıları bulunmuştur. Çalışma [175] kanal parametreleri arasındaki ilişki 781 MHz bandında MIMO sistem için incelenmiş ve ilinti katsayıları kentsel, kırsal ve banliyö gib 3 farklı ortamda elde edilmiştir. Çalışma [176] karşılıklı kanal özelliği ile anahtar üretim metodunu OFDM-FDD sisteminin CSI'ına bağlı olarak yeni bir yaklaşım sağlamışlardır. OFDM sistemlerdeki adaptif anahtar üretim tekniği çalışma [177]'de incelenmiştir.

Çalışma [178]'da, UWB kanallardaki anahtar üretim için adaptif nicemleme metodu, karşılıklı kanal özellikliği kullanılarak anlatılmıştır. [179]'de, anahtar üretimi OFDM sistemin alt-taşıyıcılarının kuantalanması için birikimli dağılım fonksiyonu kullanılmıştır. Çalışma [180]'de ise MIMO sistemlerde karşılıklı kanal durumu kullanılarak 2 farklı anahtar üretim tekniği hakkında teorik çalışmalar yapılmıştır. Çalışma [181], çok-yollu kablosuz karşılıklı kanal özelliği kullanılan anahtar üretim algoritması gerçeklenmiştir. [182] çalışmasında; bina içindeki karşılıklı kanal özelliği ve UWB için ilinti özelliği araştırılmıştır. Ayrıca bu özellikler, nicemleme algoritması kullanılan anahtar üretimi için de kullanılmıştır.

Çalışma [183], güvenli kablosuz bağlantılar için OFDM alt-taşıyıcılarının CSI kullanılan anahtar üretimi üzerinde durulmuştur. Çalışma [184], geliştirilmiş karşılıklı kanal durumuyla yapılan anahtar üretimin performans sonuçları incelenmiştir. Anahtar üretimi için, adaptif nicemleme tekniği kullanılmıştır. Çalışma [185], UWB anahtar üretim metodunun, yeni tanımlanan saldırı durumlarına karşı, bina içi karşılıklı kanal durumu ve uzaysal ilintisizleşme özelliği kullanılarak güvenliği kontrol edilmiştir. [186] çalışması için; kablosuz ağlardaki fiziksel katman güvenliği tarafından önlenen farklı saldırı türleri incelenmiş, sonrasında her bir saldırı türü içi anahtar üretimindeki hata oranı hesaplanmıştır. Çalışma [187], fiziksel katman güvenliği için anahtar üretiminde SNR ve ilinti fonksiyonu gibi kanal paremetrelerinin ve limitli kanal bilgi durumunun etkisi açıklanmıştır. Çalışma [188] OFDM sisteminde CDF tabanlı nicemleme algoritması kullanılarak anahtar üretimi açıklanmıştır.

4.8.1 İlinti Katsayısı

İlinti katsayısı 2x2 MIMO sistem için dört karşılıklı Kanal Çiftinin karşılıklı olarak birbirleriyle ilişkisini test etmek için kullanılmıştır. İlinti katsayısı değeri -1 ile 1 arasında değişkenlik göstermektedir. Karşılıklı kanallar arasında yüksek ilişki beklenmektedir. Bu da bulunan değerlerin mümkün olduğunca 1'e yakın olması gerektiği anlamına gelmektedir. İki değer arasındaki ilişki için ilinti katsayısı (ρ) formülasyonu aşağıda gösterilmiştir [165].

$$\rho(u,v) = \frac{1}{N-1}\sum_{i=1}^{N}\left(\overline{\frac{u_i-\mu_v}{\sigma_u}}\right)\left(\frac{v_i-\mu_v}{\sigma_v}\right) \tag{92}$$

Formülde kullanılan μ_u ve σ_u, sırasıyla u'nun ortalama ve standard sapma değerleriyken, μ_v

ve σ_v, sırasıyla v'nin ortalama ve standard sapma değerleridir. N ise ilinti katsayıları bulunacak olan değişkenlerin dizi uzunluğudur. Bu nedenle iki dizi birbirine uzunluk olarak eşit olmalıdır. Ayrıca, ilinti katsayısı değerleri, u ve v'nin kovaryanslarından da bulunabilir

$$\rho(u,v) = \frac{cov(u,v)}{\sigma_u \sigma_v} \tag{93}$$

4.8.2 Anahtar Üretimi ve Düzgün Nicemleme Metodu

Karşılıklı kanal özelliği kullanılarak bulunan ortalama kanal katsıyısı vektörleri h_{AB} ve h_{BA} şeklinde simgelenmiştir. $N_t \times N_r$ MIMO-OFDM sistem için $j = 1, \ldots, N_t$ ve $k = 1, \ldots, N_r$ olmak üzere h_{AB}^{jk} ve h_{BA}^{jk} gibi $N_t N_r$ adet karşılıklı kanal çifti olmak üzere 2x2 MIMO sistemimiz için, $N_t = 2$, $N_r = 2$ olduğundan bu durumda 4 tane karşılıklı kanal çifti vardır. Kanal katsayısı vektörlerinin genlik değerleri ($|h_{AB}^{jk}|$, $|h_{BA}^{jk}|$) ve faz değerleri ($\angle h_{AB}^{jk}$, $\angle h_{BA}^{jk}$) anahtar üretiminde önemli bir rol oynar. İki farklı anahtar çıkarma tekniği uygulanmıştır.

İki anahtar tekniğinin kullandığı ortak değişkenler, genlik için G_{AB} ve G_{BA}, faz için F_{AB} ve F_{BA} şu şekilde hesaplanmıştır

$$G_{AB} = \begin{bmatrix} |h_{AB}^{11}| & |h_{AB}^{12}| & |h_{AB}^{21}| & |h_{AB}^{22}| \end{bmatrix}, \tag{94}$$

$$G_{BA} = \begin{bmatrix} |h_{BA}^{11}| & |h_{BA}^{12}| & |h_{BA}^{21}| & |h_{BA}^{22}| \end{bmatrix}, \tag{95}$$

$$F_{AB} = \begin{bmatrix} \angle h_{AB}^{11} & \angle h_{AB}^{12} & \angle h_{AB}^{21} & \angle h_{AB}^{22} \end{bmatrix}, \tag{96}$$

$$F_{BA} = \begin{bmatrix} \angle h_{BA}^{11} & \angle h_{BA}^{12} & \angle h_{BA}^{21} & \angle h_{BA}^{22} \end{bmatrix}. \tag{97}$$

Her bir kanal katsayı vektörü (h_{AB}^{jk} ve h_{BA}^{jk}) uzunluğu 1x320 olmak üzere; oluşturulan genlik için G_{AB}, G_{BA} ve faz için F_{AB}, F_{BA} dizileri 1x1280 uzunlukta olacaktır. S_f değeri 1280 uzunluğuna tam bölünecek şekilde seçilmiştir. İlk teknik için, frekans ilişkisi incelendiğinde S_f ilişkili alttaşıyıcı sayısı olmak üzere, ortalamaları alınarak anahtar üretimi gerçekleştirilmiştir.

$$G_{AB}^{ort}(m) = \frac{1}{S_f} \sum_{i=(m-1)S_f+1}^{mS_f} G_{AB}(i), \tag{98}$$

$$G_{BA}^{ort}(m) = \frac{1}{S_f} \sum_{i=(m-1)S_f+1}^{mS_f} G_{BA}(i), \tag{99}$$

$$F_{AB}^{ort}(m) = \frac{1}{S_f} \sum_{i=(m-1)S_f+1}^{mS_f} F_{AB}(i), \tag{100}$$

$$F_{BA}^{ort}(m) = \frac{1}{S_f} \sum_{i=(m-1)S_f+1}^{mS_f} F_{BA}(i), \tag{101}$$

$N = 1280$ olmak üzere $i = 1, \ldots, N$ ve $m = 1, \ldots, \frac{N}{S_f}$ için ilk teknik uygulanmış ve 4 vektör bulunmuştur.

İkinci teknikte ise S_f ilişkili alttaşıyıcıları için minimumları seçilerek anahtar üretimi gerçekleştirilmiştir.

$$G_{AB}^{min}(m) = \min_{i \in \{(m-1)S_f+1, \ldots, mS_f\}} \left(G_{AB}(i)\right). \tag{102}$$

$$G_{BA}^{min}(m) = \min_{i \in \{(m-1)S_f+1, \ldots, mS_f\}} \left(G_{BA}(i)\right). \tag{103}$$

$$F_{AB}^{min}(m) = \min_{i \in \{(m-1)S_f+1, \ldots, mS_f\}} \left(F_{AB}(i)\right). \tag{104}$$

$$F_{BA}^{min}(m) = \min_{i \in \{(m-1)S_f+1, \ldots, mS_f\}} \left(F_{BA}(i)\right). \tag{105}$$

$N = 1280$ olmak üzere $i = 1, \ldots, N$ ve $m = 1, \ldots, \frac{N}{S_f}$ için ikinci teknik uygulanmış ve 4 vektör bulunmuştur.

$P \in \{G_{AB}^{ort}(m), G_{BA}^{ort}(m), F_{AB}^{ort}(m), F_{BA}^{ort}(m)\}$ ve $R \in \{G_{AB}^{min}(m), G_{BA}^{min}(m), F_{AB}^{min}(m), F_{BA}^{min}(m)\}$ ve L nicemleme örneğinin kaç bit olduğunu temsil ederken, k_{ort}, AB kanalı ile BA kanalının S_f ilişkili alıcılarının ortalamasına göre genlik ve faz için ayrı iki anahtar vektörünü, k_{min} AB kanalı ile BA kanalının S_f ilişkili alıcılarının minimumuna göre genlik ve faz için ayrı iki anahtar vektörünü içermektedir.

$$k_{ort} = f(P, L, S_f), \tag{106}$$

$$k_{min} = f(R, L, S_f), \tag{107}$$

Bu çalışmada Mid-rise nicemleme tekniği kullanılmıştır. Öncelikle kullanılması gereken nicemleme seviyesi (Q) seçilmesi gereklidir. Bu seçilen seviye, her kuantalanmış örneğe atanmış olan bit sayısını (L) belirler. Böylece toplam anahtar uzunluğu LN/S_f olacaktır. Nicemleme seviyesi ve bit sayısı arasındaki ilişki bu şekildedir $Q = 2^L$. Sonrasında, genlik genişliği (A) kuantalanacak olan vektörün minimum ve maksimum değerlerinin farkı olmak üzere hesaplanır. Son olarak, kuantalayıcının adım büyüklüğünden (Δ) hesaplanmalıdır. $\Delta = A/Q$ bu şekilde bulunur. Bu süreçten sonra, her kuantalanan örneğe atanması gereken, L'e bağlı olan bitler vardır. Üretilen bu bitler, Gray koduna göre ayarlanmalıdırlar [166]. Bu bitlerin tümü, anahtar üretimini sağlamaktadır. Her karşılıklı kanal çifti bu süreçten geçtiğinde, her çift için genlik ve faz anahtarları oluşmuş olur. Sonrasında, iki anahtar karşılaştırıldığında (genlik ve faz ayrı ayrı), anahtar hata oranına ulaşılır [167]. Bu anahtar hata oranı 0 ile 1 arasındadır.

4.8.3 Test Ortamı ve Sonuçları

Testler İTÜ Telsiz Haberleşme Araştırma Laboratuvarında gerçekleştirilmiş ve ölçüm düzeneği Şekil 34'deki ve sistem parametreleri Çizelge 5'deki gibidir.

Çizelge 5: Sistem Parametreleri

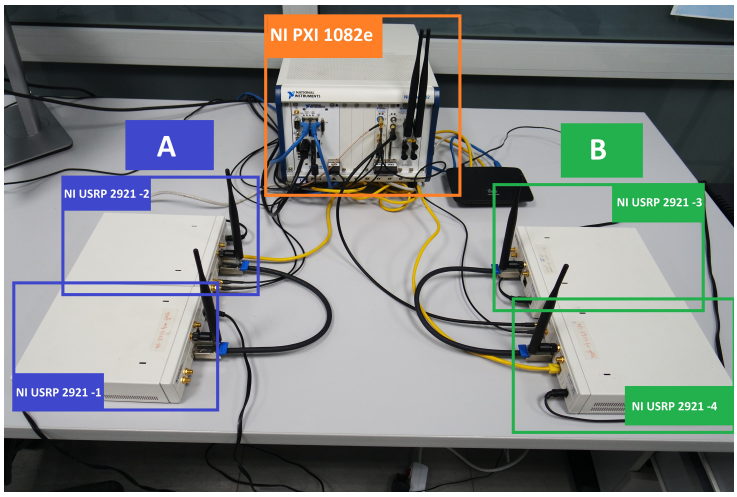
Taşıyıcı Frekans	2.45 GHz
İletim Kazancı	0/10/20/20 dB
Alıcı Kazancı	0/10/20/30 dB
I/Q Veri Oranı	1 MS/sec
Bir Çerçevedeki Bit Sayısı	640
Referans Alttaşıyıcı Sayısı	360
Zero Padding Uzunluğu	120
FFT Uzunluğu	480
Ön Ek Uzunluğu	120
Çerçevedeki Toplam Alt Taşıyıcı Sayısı	600

Dört farklı kanal kazanç durumuna göre testler yapılmıştır. A USRP birimlerinden, B USRP birimlerine toplamda 320000 kanal katsayısı, $i \in \{1, 2, ..., 1000\}$ olmak üzere dört kanal için sırayla $h^{11}_{AB,i}$, $h^{21}_{AB,i}$, $h^{12}_{AB,i}$, $h^{22}_{AB,i}$ kanal katsayısı vektörleri elde edilmiştir. B USRP birimlerinden, A USRP birimlerine de aynı işlem gerçekleştirilerek dört kanal için $h^{11}_{BA,i}$, $h^{21}_{BA,i}$, $h^{12}_{BA,i}$, $h^{22}_{BA,i}$ kanal katsayısı vektörleri elde edilmiştir.

Karşılıklı Kanal Özelliği Sonuçları Testler sonucunda elde edilen ortalama kanal katsayı vektör çiftlerinin (h^{jk}_{AB} ve h^{jk}_{BA}) genlik ve faz bilgileri gözlenmiştir. A USRP biriminden B USRP birimine olan kanal AB, B USRP biriminden A USRP birimine olan kanal BA olarak temsil edilmek üzere 4 kanalın genlik ve faz ortalama değerleri Şekil 35'de gösterilmiştir.

İlinti Katsayısı Sonuçları Elde edilen kanal katsayısı vektörleri için genlik ve faz ortalama değerlerinin 4 karşılıklı kanal çifti için ilinti katsayıları 4 farklı kazanç durumuna göre hesaplanmış ve minimum, maksimum ve ortalama değerleri Çizelge6'de gösterilmiştir.

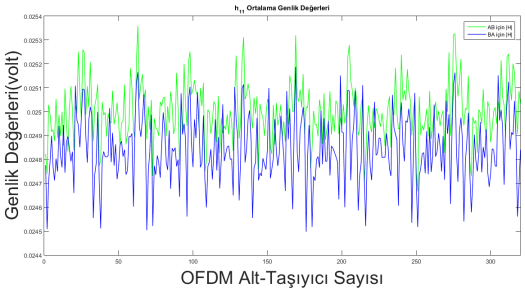
Anahtar Üretimi Sonuçları Düzgün Nicemleme metodu olan Mid-Rise tipi nicemleme, ortalama kanal katsayı vektörlerinin elde edilen genlik ve faz değerlerine uygulanmıştır. Her bir karşılıklı kanal çiftleri için, L'ye bağlı kalan iki farklı anahtar hesaplanmıştır. Bu iki anahtar karşılaştırıldığında, 4 farklı kanal kazancı durumu, 7 farklı S_f değeri için Tablo 7, Tablo 8, Tablo 9 ve Tablo 10'de ortalama genlik ve faz değerlerinden, karşılıklı kanal çiftleri için anahtar hata oranı elde edildi.



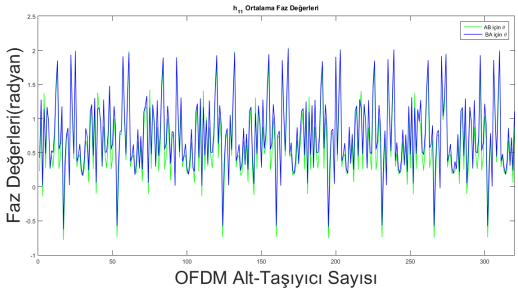
Şekil 34: Ölçüm Düzeneği

Çizelge 6: İlinti Katsayılar Tablosu

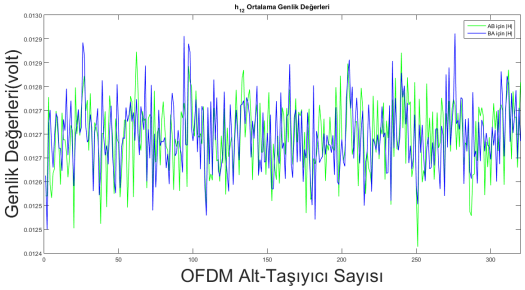
		Genlik			Faz		
$Tx-Rx$	$Kanallar$	Minimum	Maksimum	Ortalama	Minimum	Maksimum	Ortalama
0-0	h_{11}	0.7925	0.9783	0.9256	0.2406	0.9615	0.9125
	h_{12}	0.2663	0.9126	0.8875	0.456	0.9746	0.9065
	h_{21}	0.1289	0.9213	0.8732	0.3597	0.9836	0.9136
	h_{22}	0.8963	0.9888	0.9734	0.7536	0.9632	0.9256
10-10	h_{11}	0.8856	0.9963	0.9724	0.7596	0.9753	0.9428
	h_{12}	0.7512	0.9247	0.9036	0.6232	0.9015	0.8875
	h_{21}	0.2636	0.8969	0.8524	0.3562	0.9265	0.8456
	h_{22}	0.6659	0.9736	0.9369	0.7456	0.8963	0.8756
20-20	h_{11}	0.8965	0.9999	0.9623	0.8845	0.9856	0.9127
	h_{12}	0.8436	0.9563	0.9367	0.7563	0.9203	0.9012
	h_{21}	0.8886	0.9546	0.9156	0.7742	0.9423	0.9156
	h_{22}	0.9452	0.9973	0.9742	0.9123	0.9652	0.9364
20-30	h_{11}	0.8236	0.9563	0.9265	0.8897	0.9786	0.9454
	h_{12}	0.2345	0.9263	0.9126	0.3615	0.8453	0.8036
	h_{21}	0.1263	0.9456	0.9294	0.6687	0.9836	0.9086
	h_{22}	0.7589	0.9023	0.8872	0.1326	0.8598	0.7436



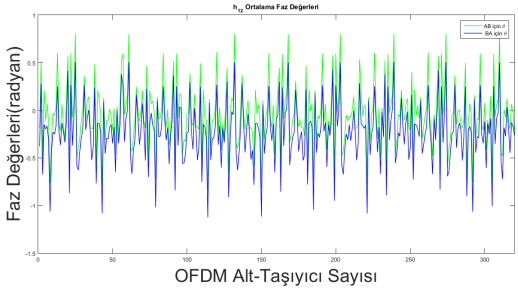
(a) $|h_{11}|$



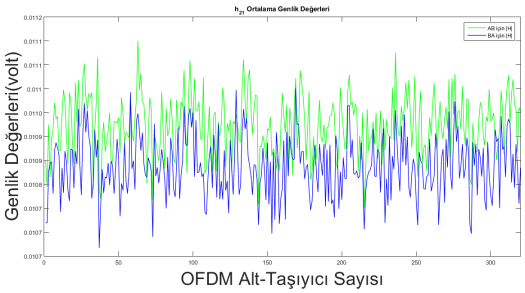
(b) $\angle h_{11}$



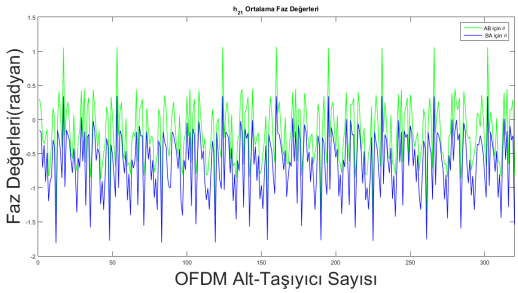
(c) $|h_{12}|$



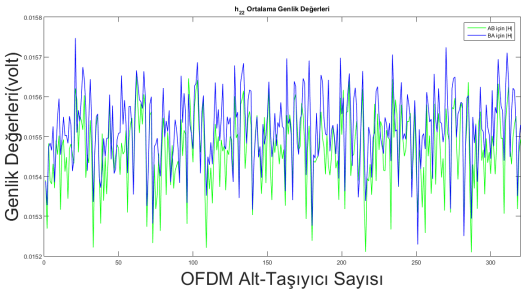
(d) $\angle h_{11}$



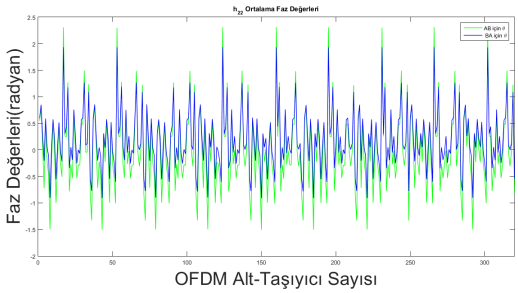
(e) $|h_{21}|$



(f) $\angle h_{21}$



(g) $|h_{22}|$



(h) $\angle h_{22}$

Şekil 35: Tx=0 dB-Rx=0 dB değerleri için dört kanalın genlik ve faz ortalamaları

Çizelge 7: Genlik ve Faz için, Tx=0 dB ve Rx=0 dB değerlerinde, değişen L ve S_f durumlarına göre bulunan KER Değerleri

			Genlik		Faz	
			S_f Ortalaması	S_f Minimumu	S_f Ortalaması	S_f Minimumu
L	S_f	Anahtar Uzunluğu	KER	KER	KER	KER
2	2	1280	0	0	0.02070	0.01734
	4	640	0.0016	0.0031	0.02688	0.02906
	8	320	0.0063	0	0.03219	0.02688
	16	160	0.0125	0.0125	0.04938	0.0300
	32	80	0.0125	0.0250	0.05125	0.03125
	64	40	0	0.0250	0.050	0.02750
	128	20	0	0	0.050	0.045
3	2	1920	0.0010	$5.2083x10^{-4}$	0.03594	0.02599
	4	960	0	0.0021	0.03990	0.03792
	8	480	0	0	0.04479	0.03938
	16	240	0	0.0083	0.03875	0.04292
	32	120	0.0083	0.0167	0.04417	0.03167
	64	60	0.0333	0.0333	0.0300	0.02667
	128	30	0	0.0667	0.0300	0.03667
4	2	2560	$3.9063x10-4$	$3.9063x10-4$	0.03625	0.3418
	4	1280	0	0.0023	0.3703	0.04063
	8	6400	0	0.0047	0.04203	0.03969
	16	320	0	0.0063	0.04563	0.04656
	32	160	0.0125	0.0063	0.03688	0.04063
	64	80	0.0250	0.0125	0.03750	0.02875
	128	40	0.0250	0.050	0.0400	0.0300
5	2	3200	0.0144	0.04438	0.1111	0.04988
	4	1600	0.0113	0.0163	0.04263	0.04544
	8	800	0.0075	0.0138	0.04650	0.05550
	16	400	0.0075	0.0150	0.0440	0.050
	32	200	0.0100	0.0100	0.04850	0.0620
	64	100	0.0100	0.0100	0.03368	0.0530
	128	50	0	0.0400	0.0400	0.0520
6	2	3840	0.0385	0.0523	0.04477	0.05005
	4	1920	0.0307	0.0557	0.04339	0.04552
	8	960	0.0125	0.0448	0.04667	0.05542
	16	480	0.0063	0.0354	0.04479	0.05104
	32	240	0.0083	0.0250	0.04792	0.06083
	64	120	0.0167	0.0167	0.03750	0.05417
	128	60	0	0.0333	0.03889	0.05333

Çizelge 8: Genlik ve Faz için, Tx=10 dB ve Rx=10 dB değerlerinde, değişen L ve S_f durumlarına göre bulunan KER Değerleri

			Genlik		Faz	
			S_f Ortalaması	S_f Minimumu	S_f Ortalaması	S_f Minimumu
L	S_f	Anahtar Uzunluğu	KER	KER	KER	KER
2	2	1280	$7.8125x10-4$	0	0.04859	0.05133
	4	640	0.0031	0.0031	0.05234	0.05578
	8	320	0	0	0.06156	0.06188
	16	160	0.0063	0.0125	0.06938	0.0550
	32	80	0	0	0.0550	0.05750
	64	40	0	0.050	0.050	0.04211
	128	20	0	0	0.0444	0.0444
3	2	1920	$5.2083x10-4$	0	0.04776	0.05156
	4	960	0.0021	0.0010	0.05375	0.05583
	8	480	0	0	0.05417	0.05667
	16	240	0.0042	0.0042	0.06042	0.05042
	32	120	0	0	0.05417	0.05083
	64	60	0	0.0333	0.04667	0.04912
	128	30	0.0333	0.0333	0.04815	0.040
4	2	2560	$7.8125x10-4$	0.0012	0.04703	0.04996
	4	1280	0.0016	0.0063	0.05320	0.05211
	8	6400	0	0.0016	0.05406	0.05625
	16	320	0	0.0063	0.05625	0.04844
	32	160	0.0063	0	0.05188	0.05375
	64	80	0	0.0250	0.04750	0.050
	128	40	0.050	0	0.05556	0.0444
5	2	3200	0.0322	0.0456	0.04825	0.05031
	4	1600	0.0200	0.0538	0.05363	0.05156
	8	800	0.0113	0.0438	0.05313	0.05588
	16	400	0.0050	0.0350	0.05375	0.04875
	32	200	0	0.0050	0.050	0.050
	64	100	0.0100	0.0300	0.0480	0.04842
	128	50	0.020	0	0.0555	0.044
6	2	3840	0.0732	0.0802	0.04854	0.05083
	4	1920	0.0688	0.0828	0.05286	0.02130
	8	960	0.0542	0.0750	0.05302	0.05594
	16	480	0.0438	0.0688	0.05375	0.04854
	32	240	0.0458	0.0542	0.04875	0.05042
	64	120	0.0583	0.0538	0.04750	0.050
	128	60	0.050	0.0667	0.05167	0.04630

Çizelge 9: Genlik ve Faz için, Tx=20 dB ve Rx=20 dB değerlerinde, değişen L ve S_f durumlarına göre bulunan KER Değerleri

			Genlik		Faz	
			S_f Ortalaması	S_f Minimumu	S_f Ortalaması	S_f Minimumu
L	S_f	Anahtar Uzunluğu	KER	KER	KER	KER
2	2	1280	0.0016	0	0.01719	0.01930
	4	640	0	0.0016	0.02469	0.025
	8	320	0	0.0031	0.03406	0.02313
	16	160	0	0.0063	0.03625	0.04438
	32	80	0	0.0250	0.045	0.04750
	64	40	0	0.05	0.0425	0.04500
	128	20	0.05	0.100	0.05	0.055
3	2	1920	0.0073	0	0.02391	0.02688
	4	960	0.0031	0.0010	0.03292	0.03406
	8	480	0	0	0.03917	0.03250
	16	240	0.0042	0.0083	0.04	0.04333
	32	120	0	0.0167	0.04833	0.05167
	64	60	0	0.0167	0.03833	0.0333
	128	30	0	0.0333	0.04667	0.03667
4	2	2560	0.0066	0.007	0.03426	0.03316
	4	1280	0.0016	0.0023	0.03828	0.03563
	8	6400	0.0031	0	0.04281	0.03453
	16	320	0.0063	0.0063	0.04438	0.04375
	32	160	0	0.0125	0.04988	0.04375
	64	80	0	0.0250	0.05625	0.03875
	128	40	0.05	0.0250	0.6250	0.04250
5	2	3200	0.0097	0.	0.03650	0.03616
	4	1600	0.0081	0.055	0.04206	0.03531
	8	800	0.0163	0.0188	0.04450	0.037
	16	400	0.03	0.0250	0.04475	0.04375
	32	200	0.05	0.0350	0.048	0.045
	64	100	0.06	0.03	0.038	0.033
	128	50	0.04	0.02	0.046	0.034
6	2	3840	0.0604	0.0602	0.05130	0.03813
	4	1920	0.0359	0.0661	0.05031	0.04781
	8	960	0.0333	0.0479	0.05177	0.05229
	16	480	0.0292	0.0563	0.05604	0.05417
	32	240	0.0458	0.0792	0.0505	0.0533
	64	120	0.0250	0.0667	0.04750	0.03417
	128	60	0.0333	0.0883	0.04833	0.041

Çizelge 10: Genlik ve Faz için, Tx=20 dB ve Rx=30 dB değerlerinde, değişen L ve S_f durumlarına göre bulunan KER Değerleri

			Genlik		Faz	
			S_f Ortalaması	S_f Minimumu	S_f Ortalaması	S_f Minimumu
L	S_f	Anahtar Uzunluğu	KER	KER	KER	KER
2	2	1280	$7.81235x10^{-4}$	$7.81235x10^{-4}$	0.03297	0.02867
	4	640	0.0031	0.0031	0.04313	0.02922
	8	320	0. 0031	0	0.050	0.03875
	16	160	0	0.0125	0.060	0.03750
	32	80	0	0.0250	0.070	0.01875
	64	40	0	0.05	0.06250	0.04750
	128	20	0	0.100	0.060	0.035
3	2	1920	$5.2083x10^{-4}$	$5.2083x10^{-4}$	0.04063	0.03448
	4	960	0	0.0021	0.04875	0.03615
	8	480	0	0.0042	0.05583	0.04146
	16	240	0	0.0083	0.05750	0.03667
	32	120	0	0.0167	0.06167	0.025
	64	60	0.0167	0	0.05500	0.04667
	128	30	0	0.0667	0.06333	0.04333
4	2	2560	0.0098	0.0109	0.04137	0.03941
	4	1280	0.0055	0.0133	0.04852	0.0418
	8	6400	0.0016	0.0078	0.05344	0.04344
	16	320	0.0031	0.0031	0.055	0.03656
	32	160	0	0.0063	0.06	0.03750
	64	80	0	0.0250	0.05625	0.040
	128	40	0	0.0250	0.6250	0.035
5	2	3200	0.0519	0. 0519	0.04275	0.04103
	4	1600	0.0413	0.055	0.04963	0.04644
	8	800	0.0388	0.0188	0.05375	0.04725
	16	400	0.0550	0.0250	0.05325	0.03875
	32	200	0.05	0.0350	0.05850	0.0345
	64	100	0.05	0.03	0.052	0.042
	128	50	0.04	0.02	0.062	0.04
6	2	3840	0.0917	0.0852	0.04398	0.04159
	4	1920	0.0839	0.0932	0.05031	0.04661
	8	960	0.0740	0.0688	0.05177	0.04750
	16	480	0.0646	0.0646	0.05229	0.03875
	32	240	0.0750	0.0750	0.05625	0.03833
	64	120	0.05	0.05	0.05	0.04583
	128	60	0.0833	0.083	0.05833	0.04167

4.9 Fiziksel katman güvenlik anahtarı çıkarımı: Anahtar hata oranı teorik analizi ve ölçüm sonuçları

Fiziksel katman bilgileri kullanılarak güvenlik anahtarı çıkarımı yapılabilir. Karşılıklı kanal özelliği (channel reciprocity), kablosuz haberleşme için kanal bilgisini kullanarak güvenlik anahatarı çıkarımı için gerekli koşulu sağlamaktadır. Elektromanyetik dalgaların tersinir özelliğine dayanan bu özellik, iki nokta arasındaki kanaldan kaynaklanan zayıflamanın her iki nokta için de benzer olup, diğer bütün noktalar için farklı olmasını sağlamaktadır. Ayrıca, bu kanal bilgisi sürekli ve rastgele bir şekilde değişmekte, bu da kanal bilgisinin başka bir nokta tarafından tekrarlanamamasını sağlamaktadır. Bu bilgiyi kullanarak oluşturulan anahatar çıkarımı metodlarına genel olarak fiziksel katman anahtar çıkarımı denir. Anahtar çıkarımı işlemsel sorunları içermemesi sebebiyle, diğer metodlara göre daha az karmaşıklık içermektedir.

Fiziksel katman anahtar çıkarım metodları genel olarak kanal bilgisinin kuantalanmasına dayanır. Bu işlem farklı sinyal işleme metodlarıyla desteklenebileceği gibi, farklı nicemleme metodlarıyla da gerçekleştirilebilir.

Her iki noktada da kanal dengeleyici kısımlarından alınan kanal katsayıları önce düzgün nicemleme (uniform quantizer) bloğundan geçirilerek, her katsayının seçilen Δ düzey aralığına göre seviyeleri belirlenir. Nicemlenen katsayılar kodlama işleminden geçirilerek bit dizileri haline getirilir. Oluşturulan bit dizilerinin birbirinin aynısı olması halinde anahtarların uyuştuğu ve güvenliğin sağlandığı söylenir. Ancak oluşturulan bit dizilerinden bir bitin bile hatalı olması halinde bitin anahtar hatalı olacağından, hatanın azaltılması önemli bir zorluk taşımaktadır.

Alice ve Bob kullanıcılarının noktadan noktaya haberleştiği düşünülecek olursa karşılıklı kanal özelliğinin kullanılabileceği gözlenebilir. Bu durumda her iki noktadaki kanal bilgisi birbirinin benzeri olacağından aynı anahtarın üretilmesi beklenmektedir. Ancak, kanal bilgisinin hatasız bir şekilde elde edilmesi mümkün değildir. Gönderim yapan noktanın bütün verilerini pilot olarak göndermesi ile kanal bilgisi her iki tarafta da benzer olabilir. Bundan dolayı, her iki noktada da gönderilen verinin arasındaki pilot işaretler kullanılarak kanal tahmini gerçekleştirilmektedir. Kanal tahmini her iki taraf için de üretilecek anahtarlar için bir hata kaynağıdır. Bu kaynağın doğru bir şekilde modellenmesi ve anahtar hata oranın (KER) belirlenmesi güvenlik sistemi tasarımı için zorunlu bir hale gelmektedir.

Bu bölümdeki çalışmada anahtar hata oranının teorik bir şekilde elde edilmesini hedeflemektedir. Kanal tahmininde oluşan hata ve nicemleme sistemi modellenerek anahtar hata orana yaklaşık bir ifade önerilmiştir. Bu ifade detaylı simülasyon ve ölçüm sonuçları ile desteklenmiştir. Böylece, sistem tasarımı sırasında seçilen parametrelere göre sistemin ne kadar hata oranı verileceği öngörülebilir olmaktadır.

4.9.1 Sistem Blokları

Kablosuz haberleşmede kanaldan kaynaklanan etki aşağıdaki gibi gösterilecek olursa;

$$y = hx + n, \tag{108}$$

h burada kanal etkisini göstermekte olup kanal dengeleyici kullanılarak gönderilen x sembollerinin geri üretilmesi hedeflenmektedir. Kanal tahmini için farklı modeller vardır. Bizim kullandığımız model X_p pilot işaretleri X sembolleri arasına belirli aralıklarla dağıtılmış olup, alıcı tarafından da bilinmektedir. Alıcı bu aralıklara denk düşen Y_p işaretlerini kullanarak kanal dengeleyicide sıfır zorlama (zero forcing) ile kanal katsayılarını belirli aralıklarla elde eder. Bu aralıklarda elde edilen katsayılar farklı yöntemlerle (lineer interpolasyon vs.) tüm kanal bilgisi yeniden oluşturulur. Bundan dolayı yeniden üretilen kanal artık $\hat{h}$ şeklinde ifade edilir. Bizim sistemimizde iki noktada da kanal tahmini yapılacağından her iki noktadaki kanal tahmini hatasının da hesaplanması gerekmektedir.

4.9.2 Anahtar Hata Oranı (KER)

Çok taşıyıcılı iki taraflı bir iletişim sistemi varsayalım. Bu sistemdeki taşıyıcı sayısı N olsun. Karşılıklı kanal özelliği dikkate alındığında, n^{th} alt taşıyıcıya denk düşen kanal katsayısı $n = 0, 1, ..., N-1$ olduğunda H_N şeklinde gösterilebilir. Alice ve Bob için kanal tahmini sonucu oluşturulan kanallar sırasıyla $\hat{H}_{n,1}$ ve $\hat{H}_{n,2}$ şeklinde ifade edilebilir. Bu durumda kanal tahmini sonuçlarını aşağıdaki gibi modelleyebiliriz;

$$\hat{H}_{n,k} = H_n + \delta_{n,k}, \tag{109}$$

$k = 1, 2$ için. Kanal tahminindeki hata olasılığı $\delta_{n,k} \sim \mathcal{CN}(0, \sigma^2_{e,k})$ şeklinde karmaşık normal dağılımlı bir şekilde tanımlanabilir.

Düzgün kuantalayıcı kullanıldığında, belirlenen Δ aralığında ve bilinen $\hat{H}_{n,1}$ ile $\mathcal{I}_l$ aralığına kuantalanan l^{th} terimi tahmin edebiliriz. $l(n) = \lfloor \frac{\hat{H}_{n,1}}{\Delta} \rfloor$ ve $\mathcal{I}_l = (l(n)\Delta, (l(n)+1)\Delta)$ şeklinde tanımlayabiliriz. Bilinen $\hat{H}_{n,1}$ için Bob'da gerçekleşen kanal tahmini sonucu $\hat{H}_{n,2} = \hat{H}_{n,1} - \delta_{n,1} + \delta_{n,2}$ şeklinde yazılabilir.

Bu sonucun genliği $|\hat{H}_{n,2}| \sim \mathcal{R}(0, \sigma^2_e)$ parametresine sahip Ricean dağılımına sahiptir. Bu parametre ise aşağıdaki gibi oluşturulabilir;

$$\sigma^2_e = \sigma^2_{e,1} + \sigma^2_{e,2}. \tag{110}$$

Ricean olasılık yoğunluk fonksiyonu kullanılarak $\Pr\left(|\hat{H}_{n,2} \in \mathcal{I}_l \middle| |\hat{H}_{n,1}|\right)$ olasılığını yani $\hat{H}_{n,2}$ kanalının $\mathcal{I}_l$ aralığında bulunma olasılığını aşağıdaki gibi ifade edebiliriz;

$$P_l = \int_{l(n)\Delta}^{(l(n)+1)\Delta} \frac{x}{\sigma^2_e} e^{-\frac{x^2+|\hat{H}_{n,1}|^2}{2\sigma^2_e}} I_0\left(\frac{x|\hat{H}_{n,1}|}{(\sigma^2_e/2)}\right) dx.$$

Yukarıdaki ifade $Q_1\left(\frac{|\hat{H}_{n,1}|}{\sigma_e}, \frac{l(n)\Delta}{\sigma_e}\right) - Q_1\left(\frac{|\hat{H}_{n,1}|}{\sigma_e}, \frac{(l(n)+1)\Delta}{\sigma_e}\right)$ şeklinde düzenlenebilir.

Bu ifade 1. kanal katsayılarının sadece belirli bir düzeyde olma olasılığını verir. Ancak 2 kanal da farklı n değerleri için farklı düzeyleri de kapsaması gerektiği için daha geniş bir ifadeye gereksinim duyulmaktadır. Bunu sağlamak için Denklem (111) eşitliğinin ilk tahmin edilen kanalın bütün değerlerini kapsayabilecek bir şekilde $|\hat{H}_{n,1}|$'in olasılık yoğunluk fonksiyonu üzerinden integralini almalıyız. İlk tahmin edilen kanal $|\hat{H}_{n,1}|$'e y diyecek olursak, tek taşıyıcılı

bir sistem için anahtar hata olasılığı, P_e, $f_Y(y)$'ye bağlı değişken bir fonksiyon haline gelir ve bu fonksiyon Denklem (119) gibi gösterilebilir.

Bütün taşıyıcılar düşünüldüğü zaman denklem aşağıdaki formu alır;

$$P_o = 1 - (1 - P_e)^N . \tag{111}$$

4.9.3 Rayleigh Sönümlemeli Kanallar

Bu kanal modeli zayıflamanın modellenmesi için en sık kullanılan model olarak sayılabilir. Bu durumda $H_n \sim \mathcal{CN}(0,1)$ olup $\hat{H}_{n,1} \sim \mathcal{CN}(0, 1+\sigma_{e,1}^2)$ şeklinde tanımlayabilir ve hata olasılığını P_e Denklem (120) gibi ifade edilebilir.

İfadenin sadeleştirilmesi için farklı metodlar vardır. İfadenin en temelinde bulunan Bessel fonksiyonunu bile kullanmak için oldukça yoğun işlem gerekmektedir. Bu nedenden dolayı $Q_1(a,b)$ ifadesi için bir yaklaşıklık aranmalıdır. Şekil 36'te de görülebileceği üzere $Q_1\left(\frac{|\hat{H}_{n,1}|}{\sigma_e}, \frac{l(n)\Delta}{\sigma_e}\right)$ ifadesinde ikinci terim $\frac{l(n)\Delta}{\sigma_e}$ her zaman için ilk terim olan $\frac{|\hat{H}_{n,1}|}{\sigma_e}$'dan küçük olacaktır. $Q_1\left(\frac{|\hat{H}_{n,1}|}{\sigma_e}, \frac{(l(n)+1)\Delta}{\sigma_e}\right)$ ifadesinde ise her zaman için ilk terim ikinci terimden küçük olacaktır. Literatürde var olan Marcum Q fonksiyonu yaklaşımları yeterli bir yaklaşıklık sağlamasına rağmen, iki giriş değerinin sadece birinin diğerinden büyük ya da küçük olduğu durumda tanımlanmaktadırlar. Bundan dolayı farklı bir yaklaşım izleyerek Marcum Q fonksiyonun içerisinde bulunan Bessel fonksiyonu üzerinden yaklaşılmıştır. $I_0(x) \approx \frac{e^x}{\sqrt{2\pi x}}$ yaklaşımı kullanılarak Denklme (112)'deki gibi bir yaklaşıklık sağlanabilir;

$$I_0\left(\frac{xy}{\sigma_e^2}\right) \approx \frac{\sigma_e}{\sqrt{2\pi xy}} e^{\frac{xy}{\sigma_e^2}} \tag{112}$$

Bu durumda Marcum Q fonksiyonlarının fark ifadesine P_m diyecek olursak P_m şağaıdaki gibi gösterilir;

$$P_m \approx \int_{l(n)\Delta}^{(l(n)+1)\Delta} \frac{x\sigma_e}{\sqrt{2\pi xy}} e^{\frac{-(x-y)^2}{2\sigma_e^2}} dx \tag{113}$$

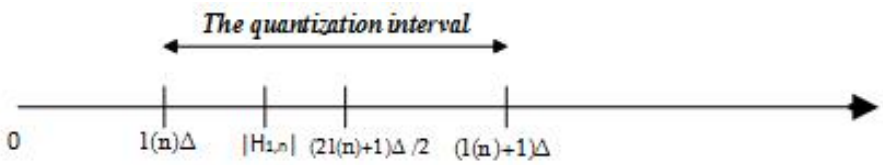
Burada $x^* = \frac{x-y}{\sigma_e}$ ve bu durumda $dx^* = \frac{dx}{\sigma_e}$ değişken dönüşümü yapıldığında ve yaklaşıklık ifadesi P_l olarak adlandırıldığında;

$$P_l = \int_{\frac{l(n)\Delta-y}{\sigma_e}}^{\frac{(l(n)+1)\Delta-y}{\sigma_e}} \frac{\sqrt{x^*\sigma_e + y}\cdot\sigma_e^2}{\sqrt{2\pi y}} e^{\frac{-x^{*2}}{2}} dx^* \tag{114}$$

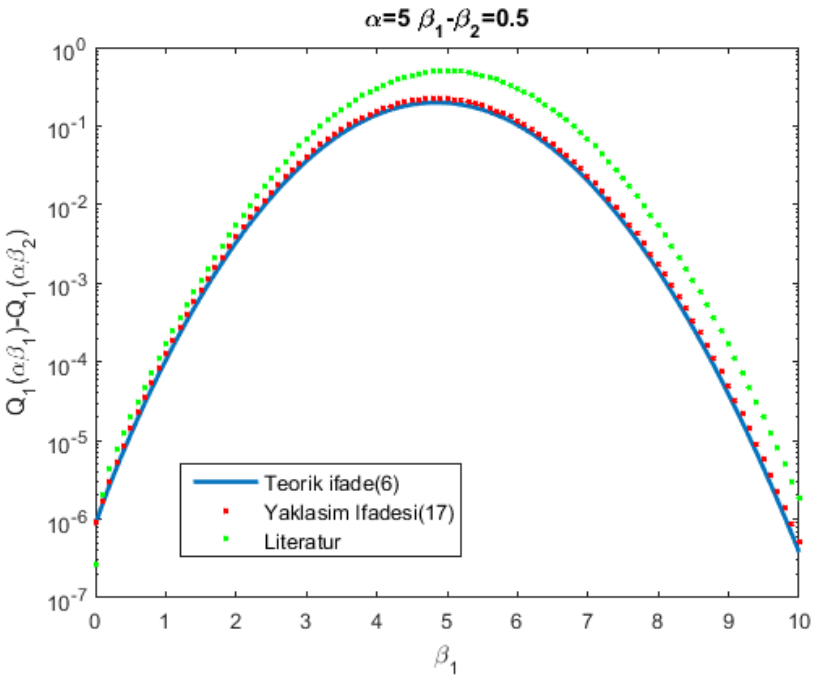
P_l ifadesi için bir üst band bulmak için Couchy-Shwartz eşitsizliği kullanılabilir. Buna göre ifade aşağıdakii gibi gösterilir:

$${P_l}^2 \leq \int_{\frac{l(n)\Delta-y}{\sigma_e}}^{\frac{(l(n)+1)\Delta-y}{\sigma_e}} \frac{\sqrt{x^*\sigma_e + y}\cdot\sigma_e^2}{\sqrt{2\pi y}} dx^* \cdot \int_{\frac{l(n)\Delta-y}{\sigma_e}}^{\frac{(l(n)+1)\Delta-y}{\sigma_e}} e^{\frac{-x^{*2}}{2}} dx^* \tag{115}$$

Şekil 37'ten de görülebileceği üzere bu ifade fark denklemi için bir üst sınır oluşturmaktadır. Her iki integral de ayrı ayrı alınıp düzenlenecek olursa Denklem (118)'e ulaşılabilir.



Şekil 36: Beklenen kuantama aralığı ve ilk kanalın tahmin edilen genliği



Şekil 37: Marcum-Q farkları ifadesinin teorik ve yaklaşım gösterimi

Bu eşitliği $f_l(y)$ fonksiyonu şeklinde tanımlayacak olursak anahtar hata oranı eşitliği aşağıdaki gibi elde edilir:

$$P_c \leq \int_0^\infty f_l(y) \cdot \frac{y}{1+\sigma_{e,1}^2} e^{-\frac{y^2}{2\left(1+\sigma_{e,1}^2\right)}} dy. \tag{116}$$

En son aşamadaki integrali çözmek için nümerik integral çözüm metodlarından birisi gerekmektedir, çünkü denklemlerin karmaşıklığı bilinen integral kurallarının dışına çıkmaktadır. Gauss-Laguerre Quadrature nümerik metodu son integralin sonucunu bulmak aşamasında önemli bir yaklaşım sağlamaktadır. Gauss-Laguerre Quadrature, Denklem (117)'deki gibi ifade edilebilir;

$$\begin{gathered} \int_0^\infty e^{-t} f(t) dt \approx \sum_{i=1}^m w_i f(t_i) \\ w_i = \frac{t_i}{(m+1)^2 [L_{m+1}^2(t_i)]} \end{gathered} \tag{117}$$

t_i Laguerre polinomu $L_m(t)$'nin i numaralı kökünü ifade etmektedir. w_i ise Laguerre ifadelerinin ağırlıklandırılmasını sağlar. Ancak bizim ifademiz şu anki halinde Gauss Laguerre Quadrature formunda değildir. İfademizin bu metodla nümerik integralini bulmak için yeniden değişken dönüşümü yapılması gerekmektedir. $\frac{y^2}{2(1+sigma_{e,1}^2)} = t$ ve $\frac{y}{(1+sigma_{e,1}^2)} = dt$ diyecek olursak;

$$P_c = \int_0^\infty f_l(\sqrt{2(1+\sigma_{e,1}^2)t}) \cdot e^{-t} dt. \tag{118}$$

$$P_e = 1 - \int_0^\infty \left[Q_1\left(\frac{y}{\sigma_e}, \frac{l(n)\Delta}{\sigma_e}\right) - Q_1\left(\frac{y}{\sigma_e}, \frac{(l(n)+1)\Delta}{\sigma_e}\right) \right] f_Y(y) dy. \tag{119}$$

$$P_e = 1 - \int_0^\infty \left[Q_1\left(\frac{y}{\sigma_e}, \frac{l(n)\Delta}{\sigma_e}\right) - Q_1\left(\frac{y}{\sigma_e}, \frac{(l(n)+1)\Delta}{\sigma_e}\right) \right] \frac{y}{1+\sigma_{e,1}^2} e^{-\frac{y^2}{2\left(1+\sigma_{e,1}^2\right)}} dy. \tag{120}$$

$$P_l' \leq \sqrt{\frac{\sqrt{\pi}}{2}\left(\frac{2\Delta^2 l(n) + \Delta^2 + \Delta}{4\pi y} + \frac{\Delta}{2\pi}\right)\left[erf\left(\frac{\Delta(l(n)+1) - y}{\sigma_e}\right) - erf\left(\frac{\Delta l(n) - y}{\sigma_e}\right)\right]} \tag{121}$$

Bu denkleme Laguerre metodu kullanılarak ifade edilmesi sonucunda anahtar hata oranı P_e aşağıdaki denkleme yaklaşıklık göstermektedir.

$$1 - \sum_{i=1}^{m} A.B \tag{122}$$

Burada A ve B aşağıdaki gibi tanımlanmıştır: olarak tanımlanmıştır.

$$A = 1 - \sum_{i=1}^{m} \left(\frac{t_i}{(m+1)^2 [L_{m+1}^2(t_i)]} \right) \tag{123}$$

$$B = \sqrt{\frac{\sqrt{\pi}}{2} \left(\frac{2\Delta^2 l(n) + \Delta^2 + \Delta}{4\pi\sqrt{2(1+\sigma_{e,1}^2)t_i}} + \frac{\Delta}{2\pi} \right) \left[erf\left(\frac{\Delta(l(n)+1) - \sqrt{2(1+\sigma_{e,1}^2)t_i}}{\sigma_e} \right) - erf\left(\frac{\Delta l(n) - \sqrt{2(1+\sigma_{e,1}^2)t_i}}{\sigma_e} \right) \right]} \tag{124}$$

4.9.4 Sayısal benzetim sonuçları

Simülasyonlarda Alice ve Bob arasındaki kanal Rayleigh modeline uygun olarak kabul edilmiştir. Her iki kanalın da kanal tahmininden kaynaklanan hataları modellemek için kompleks normal dağılımlı farklı gürültüler oluşturulup bunlar kanala eklenmiştir. Ardından her iki kanal için de düzgün nicemleme işlemi yapılmış ve kuantalanan seviyelerin eşleşmelerine göre anahtar hata oranı sonucu çıkarılmıştır.

KER sonuçları Monte Carlo metodu kullanılarak oluşturulmuşlardır. Hem grafiklerden hem de teorik çıkarım ifadelerinden anlaşılacağı üzere nicemleme aralığı ve kanal tahmini hatalarının standart sapma değerleri, anahtar hata oranını belirleyen en temel faktörlerdir. Δ'nın standard sapmalara oranı sistemin güvenilirliğini oluşturmada dikkat edilmesi gereken bir parametre olarak göze çarpmaktadır. Bu oran yükseldikçe KER değerinin düştüğü Şekil 38 den de gözlemlenebilir.

Simülasyon sonuçları ve elde edilen analizlerin de gösterdiği üzere, her iki kanalın da kanal tahmininden kaynaklı standart sapması aynı etkiyi göstermemektedir. Alıcı düğümü vericinin kanaldan etkilenmiş bir biçimde gelen anahtar ile karşılaştırma yapacağından dolayı, 1. kanalın standart sapması ifadede daha etkili olacaktır.

4.9.5 Test Ortamı ve Ölçüm Sonuçları

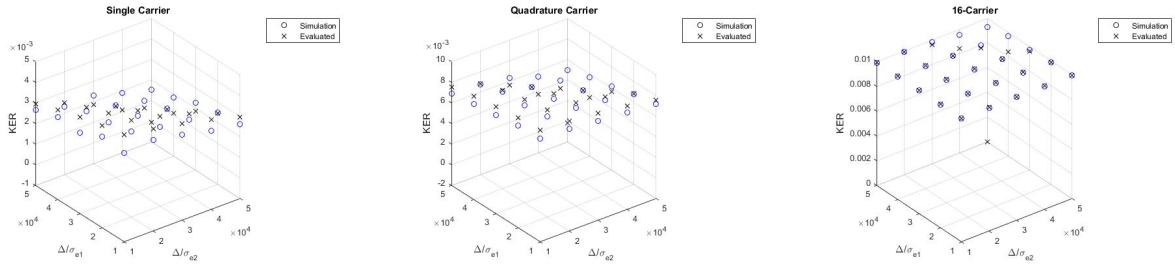
Ölçümler İTÜ Elektronik ve Haberleşme Bölümü, Telsiz Haberleşme Laboratuvarında gerçekleştirilmiştir. USRP NI- 2921 yazılım tabanlı radyoları kullanılarak ölçümler gerçekleştirilmiştir. Yazılım tabanlı radyolar LabVIEW yazılımı üzerinden kontrol edilip, programlanabilmektedirler.

MIMO düzeneği Şekil 34'deki gibidir. İki USRP gönderici, iki USRP alıcı düğüm olarak kullanılmaktadır. Taşıyıcı frekansı 2.45 GHz olarak seçilmiştir. OFDM çoğullama metodu olarak seçilmiş olup, quadrature faz kaydırmalı anahtarlama (QPSK) modülasyonu Çizelge 5'deki verilen diğer parametreler seçilerek kullanılmıştır.

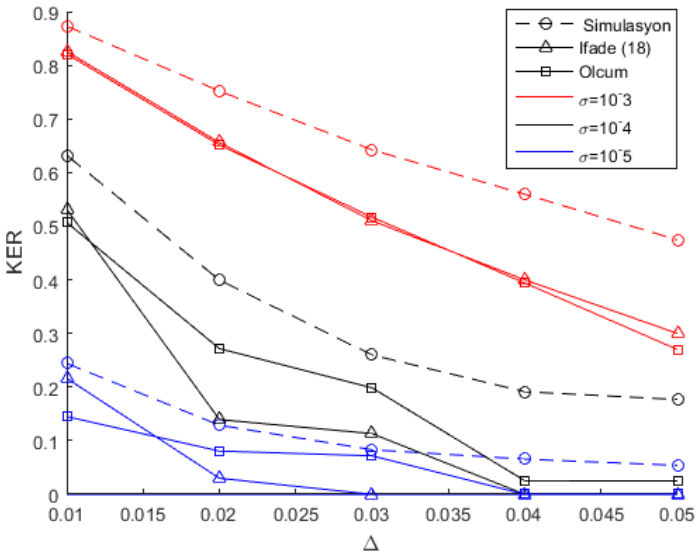
Ölçümler gerçekleştirilirken NI PXI-6683 modülü senkronizasyon amaçlı kullanılmıştır. Bu modül master saatten GPS yardımı ile 10 MHz'lik bir saat işareti üretmektedir. Bu saat işareti PPS kabloları aracılığı ile birer alıcı ve verici birimlerine iletilmekte ve iletimin kontrolü sağlanmaktadır. OFDM çoğullama metodu güçlü bir senkronizasyona ihtiyaç duyduğundan dolayı bu modülün kullanımı zorunludur. Diğer alıcı ve verici USRPleri şekilde de görülebileceği üzere MIMO kablosu ile saat işaretini almaktadırlar.

Yukarıda anlatılan ortamda ölçümler yapılmış olup, A düğümünden B düğümüne bütün işaretler pilot olacak şekilde gönderim yapılmıştır. H kanalının sıfır zorlayıcı (ZF) ile tamamen elde edildiğini düşünebiliriz. Bu kanal katsayılarının genlik değerlerinden en az Monte Carlo simülasyonunu gerçekleştirebilecek kadar örnek alınmıştır. Alınan kanal katsayılarının genlikleri $f_y(y)$ fonksiyonu yerine konarak integral ifadesi 0'dan sonsuza toplam şekline çevrilmiştir. Aslında simülasyon ve teorik çıkarımdaki gibi kanal katsayılarının genlikleri için Rayleigh dağılımını kullanmak yerine doğrudan ölçülen kanal bilgisi kullanılmıştır.

Şekil 39 bütün ölçüm, simülasyon ve değişkenlerin girilmesiyle üretilen sonuçların kıyaslamasını göstermektedir. Şekilde iki cihazın kanal tahmini standart sapmaları birbirlerine eşit kabul edilmiş olup, farklı Δ ve σ_e değerlerinin karşılaştırılması görülmektedir. Bu şekil özellikle anahtar çıkarımı için hem simülasyon hem de gerçek kanal ölçüm değerlerine yakın bir hata tahmin ifadesinin üretilebileceğini göstermesi sebebiyle önemlidir. Böylece sadece belirli parametrelerde değişiklik yapılarak, hata oranı kolayca öngörülebilecektir. Bunun yanısıra sadece nicemleme aralığının optimal seçilmesi sistemin başarısı için yeterli olmayıp, bu aralığın standart sapmaya göre seçilmesi gerektiği de gözlemlenmektedir.



Şekil 38: Farklı taşıyıcı sayılarına göre KER değerleri



Şekil 39: Ölçüm-simülasyon ve teorik çıkarım değerlerinin karşılaştırması

5 Tartışma ve Sonuç

Proje kapsamında kablosuz haberleşme sistemleri için farklı senaryolar gözönüne alınarak verimli bir fiziksel katman güvenliği yöntemi tasarlanması amaçlanmıştır. Bu amaç doğrultusunda durağan ve durağan olmayan kanallarda güvenli MISO ve MIMO tabanlı sistemler gözönünde bulundurularak tasarlanan algoritmaların başarımları bilgisayar benzetimi ile ve deneysel olarak incelenmiştir.

Durağan kanallar için güvenli MISO sistemi birden fazla antenli verici, tek antenli birden fazla aktif kullanıcı arasından seçilen tek yetkili kullanıcı ve birden fazla antenli gizli dinleyici içermektedir. Bu güvenli MISO sistemi için eşik değerine dayalı kullanıcı seçimi yapılarak güvenlik kapasitesinde kayıp olmadan nicemlenmiş kanal yön bilgisi için geri besleme yükü önemli ölçüde azaltılmıştır. Yetkili kullanıcıdaki bu seçim kriterinin gizli kullanıcının pasif dinleyici ve aktif dinleyici olduğu durumlar için güvenlik performansı üzerine etkileri incelenmiştir. Durağan olmayan kanallar için güvenli MISO sistemi birden fazla antenli verici, tek antenli tek yetkili kullanıcı ve birden fazla antenli gizli dinleyicisine sahiptir. Bu güvenli MISO sistemi için kanal yön bilgisi diferansiyel kod kitapçığı kullanılarak nicemlenmiş ve güvenlik kapasitesinin zamanla azalması önlenmiştir.

Güvenli MISO-OFDM sistemi birden fazla antenli verici, tek antenli tek yetkili kullanıcı ve tek antenli tek gizli dinleyicisine sahiptir. Bu güvenli MISO-OFDM sistemi için alttaşıyıcı kümelerinin sınıflandırılması, her alttaşıyıcı kümesi için kablosuz kanalın faz bilgisinin döndürülmüş kod kitapçığı kullanılarak nicemlenmesi ve bilginin gizli alıcılar tarafından sezinlenme olasılığı azaltmak için hüzmeleme vektörünün belirlenmesi ile uzamsal imzaya dayalı model geliştirilmiş ve güvenlik kapasitesi arttırılmıştır.

Güvenli çoklu kullanıcılı MISO sistemi birden fazla antenli verici, tek antenli seçilen birden fazla yetkili kullanıcı ve tek antenli tek gizli dinleyici içerir. Bu güvenli MISO sistemi için yetkili kullanıcı tarafında yarı-dik kriterine dayalı kullanıcı seçimi yapılmış ve döndürülmüş kod kitapçığı kullanılarak nicemlenmiş kanal yön bilgisi elde edilmiştir. Nicemlenmiş kanal yön bilgisi sebebiyle verici tarafında seçilen birden fazla yetkili kullanıcı arasında karışım oluşmaktadır ve bu karışım gizli dinleyicinin algısını bozmaktadır. O nedenle yapay gürültü modeli bu sistemde uygulanmamakta olup gücün tamamı yetkili kullanıcılar için kullanılmaktadır. Yarı dikgen tabanlı kullanıcı seçimi kullanılarak da kanal koşulları zayıf olan kullanıcıların kanal durum bilgilerinin vericide olması engellenerek sistem yükü önemli oranda düşürülmüştür. Öte yandan, yarı dikgen tabanlı seçim algoritmasının özelliklerinden yararlanılarak döndürülmüş kod kitapçığı tasarlanmıştır. Döndürülmüş kod kitapçığının ise, özellikle düşük nicemleme bitleri için güvenlik kapasitesini önemli ölçüde arttırdığı gösterilmiştir. Bu kazanç fiziksel katmanda güvenlik sistemlerinin kanal kestirim hatasına dayanlıklılığını arttırılmasına yol açmaktadır.

Güvenli çoklu kullanıcılı MIMO sistemi birden fazla antenli verici, tek antenli seçilen birden fazla yetkili kullanıcı ve tek antenli işbirliği olan birden fazla gizli dinleyici içerir. Birden fazla gizli dinleyicisi olduğu için yetkili kullanıcılar arasındaki karışım aralarında işbirliği yapan gizli dinleyiciler tarafından yok edilmektedir.Bu sebep ile yapay gürültüye gizli dinleyicinin algısını bozmak için güç paylaşımı yapılmaktadır. Bu güvenli MIMO sistemi için de yarı-dik kriterine dayalı kullanıcı seçimi yapılmış, döndürülmüş kod kitapçığı uygulanmış ve böylece hem güven-

lik kapasitesi arttırılmış hem de geri besleme yükü önemli ölçüde azaltılmıştır.

MIMO-OFDM sistemlerinde pre-FFT hüzmeleme tekniği yazılım tabanlı radyolarda gerçekleştirilmiş, en iyi hata performansı, istenilen BER ve EVM değerlerine hüzmeleme katsayılarının uygun açı durumlarında ulaşıldığı gösterilmiştir. Bu çalışma, hüzmeleme yöntemi ile fiziksel katman güvenliği için yeni yapıların oluşturulmasını kolaylaştıracaktır.

Hem SISO-OFDM hem MIMO-OFDM sistemler için yazılım tabanlı radyo teknolojisi ile karşılıklı kanal özelliği incelenmiştir. Elde edilen sonuçlar, hem grafiksel olarak kanal davranışlarının birbirine benzer olduğu göstermekte hem de ilinti katsayısıyla incelenen karşılıklı kanalların 1 değerine çok yakın yani birbirine benzer çıktığı sonucunu vermektedir. Karşılıklı kanal özelliği, fiziksel katman güvenlik anahtarı oluşturma işlemi için verimli bir kaynak olarak değerlendirilerek farklı kazanç durumları için karşılıklı kanallar Mid-rise nicemleme yöntemi ile güvenlik anahtar üretimi yapılmıştır. Üretilen bu anahtarlar karşılaştırıldığında elde edilen anahtar hata oranı birçok durum için düşük değerler almış, bazı durumlar için ise 0 değerine sahip olduğu gözlenlenmiştir. Yazılım tabanlı radyolardan ölçülen gerçek kanal değerleri ile elde edilen anahtar hata oranları, anahtar uzunluğu ve kanal kestirim hatasına göre teorik olarak elde edilen matematiksel ifadeler ile karşılaştırılarak, yakın bir hata tahmin ifadesinin üretilebileceği gösterilmiştir.

Kaynaklar

[1] Narayan S., Feng T., Xu X., Ardham S. 2009. "Impact of Wireless IEEE802.11n Encryption Methods on Network Performance of Operating Systems", Int'l. Conf. on Emerging Trends in Engineering and Technology (ICETET), pp.1178-1183.

[2] Jingfeng Y., Fang Q., Li Y., Chen H. 2011 "The random parameters insertion encryption methods of LBS application based on RSA algorithms", Int'l. Conf. on Remote Sensing, Environment and Transportation Engineering (RSETE), pp.5542-5545.

[3] Zibideh W.Y., Matalgah M.M. 2011. "Modified-DES encryption algorithm with improved BER -performance in wireless communication", IEEE Radio and Wireless Symposium (RWS), pp.219-222.

[4] Mathur C.N., Subbalakshmi K.P. 2006. "NIS05-5: Energy Efficient Wireless Encryption", IEEE Global Telecommunications Conference, pp.1-5.

[5] Narayan S., Kolahi S.S., Sunarto Y., Nguyen D.D.T., Mani, P. 2008. "The Influence of Wireless 802.11g LAN Encryption Methods on Throughput and Round Trip Time for Various Windows Operating Systems", Communication Networks and Services Research Conference (CNSR), pp.171-175.

[6] Huang J., Zheng Z., 2010. "A method for secure real-time image transmission based on optical encryption", Int'l. Symp. on Intelligent Signal Processing and Communication Systems (ISPACS), pp.1-4.

[7] Hamalainen P., Heikkinen J., Hannikainen M., Hamalainen T.D. 2005. "Design of transport triggered architecture processors for wireless encryption", Proceedings of Euromicro Conference on Digital System Design, pp. 144-152.

[8] Narayan S., Feng T., X. Xu, Ardham S. 2009. "Network performance evaluation of wireless IEEE802.11n encryption methods on Windows Vista and Windows Server 2008 operating systems", IFIP Int'l. Conf. on Wireless and Optical Communications Networks (WOCN), pp.1-5.

[9] Nanjunda C., Haleem M.A., Chandramouli R. 2005. "Robust encryption for secure image transmission over wireless channels", IEEE Int'l. Conf. on Communications (ICC), vol.2, pp. 1287-1291.

[10] Haleem M.A., Mathur C.N., Chandramouli R., Subbalakshmi K.P. 2007. "Opportunistic Encryption: A Trade-Off between Security and Throughput in Wireless Networks", IEEE Trans. on Dependable and Secure Computing, 4-4, pp.313-324.

[11] Jokar P., Nicanfar H., Leung V.C.M. 2011. "Specification-based Intrusion Detection for home area networks in smart grids", IEEE Int'l. Conf. on Smart Grid Communications (SmartGridComm), pp.208-213.

[12] Avishai W. 2005. "Lightweight key management for IEEE 802.11 wireless LANs with key refresh and host revocation", Wireless Networks, 677-686.

[13] Khisti A., Wornell G. 2010. “Secure transmission with multiple antennas Part II: the MIMOME wiretap channel,” IEEE Trans. Inf. Theory, vol. 56, no. 11, pp. 5515-5532.

[14] Alves, H., Souza, R.D., Debbah, M., Bennis, M. 2012. "Performance of Transmit Antenna Selection Physical Layer Security Schemes", IEEE Signal Processing Letters, 19-6, pp.372-375.

[15] Trappe W., LIU R. 2009. "Securing Wireless Communications at the Physical Layer", 1 st ed. Springer Publishing Company, Incorporated.

[16] Wyner A. D. 1975. "The Wire-tap Channel", The Bell System Technical Journal, vol. 54, pp. 1355-1387.

[17] Csiszar I., Korner J. 1978. "Broadcast Channels with Confidential Messages", IEEE Trans. on Info. Theory, vol. 24, pp. 339-348.

[18] Gopala P., Lai L., El Gamal H. 2008. “On the secrecy capacity of fading channels,” IEEE Trans. Inf. Theory, vol. 54, no. 10, pp. 4687–4698.

[19] Liu T., Shamai S. 2009. "A note on the secrecy capacity of the multiple-antenna wiretap channel", IEEE Trans. Inf. Theory, vol. 55,no. 6, pp. 2547–2553.

[20] Oggier F., Hassibi B. 2011.i "The secrecy capacity of the MIMO wiretap channel", IEEE Trans. Inf. Theory, vol. 57, no. 8, pp. 4961–4972.

[21] Sarkar M.Z.I., Ratnarajah T., Sellathurai M. 2009. "Secrecy capacity of Nakagami-m fading wireless channels in the presence of multiple eavesdroppers", Signals, Systems and Computers, Conference Record of the Forty-Third Asilomar Conference on, pp.829-833.

[22] Gopala P.K., Lifeng L, Hesham E. G. 2007. "On the Secrecy Capacity of Fading Channels", IEEE Int’l. Symp. Info. Theory, pp.1306-1310.

[23] Bagherikaram, G., Motahari, A.S., Khandani, A.K. 2009. "Secrecy capacity region of Gaussian broadcast channel", Conf. Info. Sci.and Sys, pp.152-157.

[24] Sarkar, M.Z.I., Ratnarajah, T. 2011. "Secrecy capacity and secure outage performance for Rayleigh fading SIMO channel", IEEE Int’l. Conf. on Acoustics, Speech and Signal Processing (ICASSP), pp.1900-1903.

[25] Noubir, G. 2004. "On Connectivity in Ad Hoc Network Under Jamming Using Directional Antennas and Mobility", Int. Conf. Wired and Wireless Internet Commun., pp. 54-62.

[26] Goel S., Negi R. 2008."Guaranteeing secrecy using artificial noise", IEEE Trans. Wireless Commun., vol. 7, no. 6, pp. 2180-2189.

[27] Liao W-C., Chang T.-H., Ma W.-K., Chi C.-Y. 2010. "Joint Transmit Beamforming and Artificial Noise Design for QoS Discrimination in Wireless Downlink", IEEE Int. Conf. on Acoustics Speech and Signal Processing (ICASSP), pp. 2562 -2565.

[28] Wu C.-Y., Lan P.-C., Yeh P.-C., Lee C.-H. , Cheng C.-M. 2013. "Practical Physical Layer Security Schemes for MIMO-OFDM Systems Using Precoding Matrix Indices",IEEE Journal on Selected Areas in Communications, vol. 31, no. 9.

[29] Parada P., Blahut R. 2005. "Secrecy capacity of SIMO and slow fading channels", in Proc. IEEE ISIT.

[30] Li Z., Trappe W., Yates R. 2007 "Secret Communication via Multi-Antenna Transmission", Conf. Info. Sci.and Sys., pp. 905-10.

[31] Shafiee S. and Ulukus S. 2007. "Achievable rates in Gaussian MISO channels with secrecy constraints", in Proc. IEEE ISIT, Nice, France.

[32] Shafiee S., Liu N., Ulukus S. 2009. "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel", IEEE Trans. Inf. Theory, vol. 55, no. 9, pp. 4033-4039.

[33] Khisti A. , Wornell G., Wiesel A., Eldar Y. 2007. "On the Gaussian MIMO wiretap channel", in Proc. IEEE Int. Symp. on Inf. Theory, pp. 2471-2475.

[34] Oggier F., Hassibi B. 2008. "The secrecy capacity of the MIMO wiretap channel", in Proc. IEEE Int. Symp. on Inf. Theory, pp. 524-528.

[35] Negi R, Goel S. 2005. "Secret communication using artificial noise", in Proc. IEEE Veh. Tech. Conf., vol. 3, pp. 1906-1910, Dallas.

[36] Khisti A., Wornell G. 2010. "Secure transmission with multiple antennas I: the MISOME wiretap channel", IEEE Trans. Inf. Theory, vol. 56,no. 7, pp. 3088-3104.

[37] Mukherjee A., Swindlehurst A.L .2009. "Fixed-rate power allocation strategies for enhanced secrecy in MIMO wiretap channels", in Proc. IEEE SPAWC, pp. 344-348, Perugia.

[38] Li Q., Ma W.-K. 2013. "Spatially selective artificial-noise aided transmit optimization for MISO multi-Eves secrecy rate maximization", IEEE Trans. Signal Process., vol. 61, no. 10, pp. 2704-2717.

[39] Gerbracht S., Scheunert C., Jorswieck E.A. 2012. "Secrecy outage in MISO systems with partial channel information", Information Forensics and Security, IEEE Transactions on, 7(2):704–716.

[40] Lin P.-H., Lai S.-H. , Lin S.-C. , Su H.-J. 2013 "On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels", IEEE J. Sel. Areas Commun., vol. 31, no. 9, pp. 1728-1740.

[41] Zhou X., McKay M. R. 2010. "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation", IEEE Trans. Veh. Technol., vol. 59, no. 8, pp. 3831–3842.

[42] Renna F., Laurenti N., Poor H.V. 2012. "Physical-Layer Secrecy for OFDM Transmissions Over Fading Channels", Information Forensics and Security, IEEE Transactions on , vol.7, no.4, pp.1354,1367.

[43] Akitaya T., Asano S., Saba T. 2014. "Time-domain artificial noise generation technique using time-domain and frequency-domain processing for physical layer security in MIMO-OFDM systems", IEEE International Conference on Communications (ICC) Workshops, pp.807-812.

[44] Bloch M., Barros J, Rodrigues,M. R. D., McLaughlin,S. W. 2008. "Wireless Information-Theoretic Security", IEEE Trans. on Info. Theory, pp. 2515-34.

[45] Cepheli, Ö., Karabulut Kurt G. 2012. "Effects of Channel Estimation Error in AN-Aided Beamforming", European Conf. on the Use of Modern Information and Communication Technologies (ECUMICT).

[46] Zhu J., Xiaohong J., Yuezhi Z., Yaoxue Z., Takahashi O., Shiratori N. 2012. "Outage performance for secure communication over correlated fading channels with partial CSI". In Services Computing Conference (APSCC), 2012 IEEE Asia-Pacific, pp. 257–262.

[47] Yang S., Piantanida S., Kobayashi M., Shamai S. 2011. "On the secrecy degrees of freedom of multi-antenna wiretap channels with delayed CSIT," 2011 IEEE International Symposium on Information Theory Proceedings, St. Petersburg, pp. 2866 - 2870.

[48] Lin S.-C., Chang T.-H. , Liang Y.-L., Hong Y.P., Chi C.H. 2011. "On the impact of quantized channel feedback in guaranteeing secrecy with artificial noise: The noise leakage problem, Wireless Communications", IEEE Transactions on, vol. 10, no:3, pp.901 - 915.

[49] Liao W., Chang T. , Ma W. , Hi C. 2011. "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach", IEEE Transactions on Signal Processing, vol. 59, no:3,pp.1202 – 1216,.

[50] Xiang H., Yener A., 2010 "Providing secrecy irrespective of eavesdropper's channel state". In Global Telecommunications Conference (GLOBECOM 2010) IEEE, pages 1–5.

[51] Wang H.-M., Luo M., Xia X.-G. , Yin Q. 2013. "Joint cooperative beamforming and jamming to secure AF relay systems with individual power constraint and no eavesdropper's CSI", Signal Processing Letters, IEEE, vol. 20, no:1, pp. 39–42.

[52] Sayeed A., Perrig A. 2008. "Secure wireless communications: Secret keys through multipath,in Acoustics", Speech and Signal Processing (ICASSP) IEEE International Conference on, pp.3013-3016.

[53] Shannon C. 1949. "Communication theory of secrecy systems", Bell Syst. Tech. J., vol. 29, pp. 656–715.

[54] Diffie W., Hellman M. E. 1976. "New directions in cryptography", IEEE Transactions on Information Theory, vol. 22, no:6, pp.644-654.

[55] Maurer U.M. 1993. "Secret key agreement by public discussion from common information",Information Theory, IEEE Transactions on , vol.39, no.3, pp.733,742.

[56] Jana S., Premnath S.N., Clark M., Kasera S.K., Patwari N., Krishnamurthy, S.V. 2009. "On the effectiveness of secret key extraction from wireless signal strength in real environments". In Proceedings of the 15th annual international conference on Mobile computing and networking (MobiCom). ACM, New York, NY, USA, 321-332.

[57] Patrawi N., Croft J., Jana S., Kasera S.K. 2010. "High-Rate Uncorrelated Bit Extraction for Shared Secret Key Generation from Channel Measurements", Mobile Computing, IEEE Transactions on , vol.9, no.1, pp.17,30.

[58] Ali S.T., Sivaraman V. 2013. "Methodologies of Secret-Key Agreement Using Wireless Channel Characteristics", DOI: 10.3969/j. issn. 1673-5188.

[59] YE C., Mathur S., Reznik A., Shah Y., Trappe W., Mandayam N.B. 2010. "Information-Theoretically Secret Key Generation for Fading Wireless Channels", Information Forensics and Security, IEEE Transactions on , vol.5, no.2, pp.240-254.

[60] Kituara A. , Sasaoka H.2005. "A Scheme of Private Key Agreement Based on the Channel Characteristics in OFDM Land Mobile Radio", Electronics and Communications in Japan, Part 3 (Fundamental Electronic Science), vol 88, No 9, p.1-10.

[61] Shehadeh E.H.Y., Alfandi O., Tout K., Hogrefe D. 2011. "Intelligent mechanisms for key generation from multipath wireless channels", Wireless Telecommunications Symposium (WTS), pp.1-6.

[62] Mathur S., Trappe W., Mandayam N. B., Ye C., Reznik A. 2008. "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel", In ACM MOBICOM Conference.

[63] Tope M. A., McEachen,J. C.2001. "Unconditionally secure communications over fading channels", In Military Communications Conference (MILCOM), vol.1, pp. 54–58.

[64] Aono T., Higuchi K., Ohira T., Komiyama B., Sasaoka H. 2005. "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels" IEEE Transactions on Antennas and Propagation, vol. 53, no:11, pp.3776–3784.

[65] Sadjadi B. A.,Kiayias A., Mercado A., Yener, B. 2007., "Robust key generation from signal envelopes in wireless networks", In Proceedings of the 14th ACM conference on Computer and communications security, pp.401–410.

[66] Brassard G., Salvail L. 1994. "Secret key reconciliation by public discussion" Lecture Notes in Computer Science, vol.765, pp. 410–423.

[67] Renna F., Laurenti N., Tomasin S., Baldi M., Maturo N., Bianchi M., Chiaraluce F., Bloch M. 2013. "Low-power secret-key agreement over OFDM". In Proceedings of the 2nd ACM workshop on Hot topics on wireless network security and privacy.

[68] Liu Y. , Draper S. ,Sayeed A. 2012. "Exploiting channel diversity in secret key generation from multipath fading randomness", IEEE Transactions on Information Forensics and Security, vol.7,pp.1484 - 1497.

[69] Dodis Y. , Reyzin L., Smith A. 2004. "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data", In Advances in Cryptology (EUROCRYPT).

[70] Ye C. Reznik A., Shah Y. 2006. "Extracting Secrecy from Jointly Gaussian Random Variables", Information Theory, IEEE International Symposium on, pp.2593,2597.

[71] Wang Q., Su H., Ren K.,Kim K. 2011. "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," INFOCOM, 2011 Proceedings IEEE , vol., no., pp.1422,1430.

[72] Zang Li, Wenyuan Xu, Rob Miller, and Wade Trappe. 2006. Securing wireless systems via lower layer enforcements. In Proceedings of the 5th ACM workshop on Wireless security (WiSe). ACM, New York, NY, USA, 33-42,(2006).

[73] Liu H., Yang W., Yang J., Yingying C. 2013. "Fast and practical secret key extraction by exploiting channel response" INFOCOM,pp.3048-3056.

[74] Ye C., Reznik A., Sternberg G., Shah, Y. 2007. "On the Secrecy Capabilities of ITU Channels", Vehicular Technology Conference (VTC-Fall), pp.2030-2034.

[75] Hershey J.E., Hassan A.A., Yarlagadda R. 1995. "Unconventional cryptographic keying variable management", Communications, IEEE Transactions on , vol.43, no.1, pp.3-6.

[76] Hassan A. A. , Stark W. E. , Hershey J.E. , Chennakeshu S. 1996. "Cryptographic Key Agreement for Mobile Radio", Digital Signal Processing, vol.6, pp.207-212.

[77] Koorapaty H., Hassan A.A., Chennakeshu S. 2000. "Secure information transmission for mobile radio," in Communications Letters, IEEE , vol.4, no.2, pp.52-55.

[78] Liu H., Yang J., Wang Y., Chen Y. 2012. "Collaborative secret key extraction leveraging Received Signal Strength in mobile wireless networks," INFOCOM, Proceedings IEEE , pp.927,935.

[79] Premnath S. N., Jana S. , Croft J., Gowda P.L., Mike Clark, Kasera S.K., Patwari N., Krishnamurthy S. V. 2013. "Secret Key Extraction from Wireless Signal Strength in Real Environments", IEEE Transactions on Mobile Computing, vol. 12, no. 5, pp. 917-930.

[80] Croft J., Patwari N., Kasera S.K. 2010. "Robust uncorrelated bit extraction methodologies for wireless sensors", In Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN), New York, NY, USA, pp.70-81.

[81] Zeng K., Wu D., Chan A.J., Mohapatra P. 2010. "Exploiting Multiple-Antenna Diversity for Shared Secret Key Generation in Wireless Networks", INFOCOM, pp.1837-1845.

[82] Quist B., Jensen M.A. 2013. "Maximizing the Secret Key Rate for Informed Radios under Different Channel Conditions" IEEE Transactions on Wireless Communications, vol.12, no.10,pp. 5146-5153.

[83] Liu Y., Draper S.C., Sayeed A.M. 2011. "Secret key generation through OFDM multipath channel", Information Sciences and Systems (CISS), 45th Annual Conference on, pp.1-6.

[84] Wallace, J.W., Chan C., Jensen, M.A.2009. "Key generation exploiting MIMO channel evolution: Algorithms and theoretical limits, Antennas and Propagation" (EuCAP) 3rd European Conference on, pp.1499-1503.

[85] Wallace, J.W., Sharma R.K.2010. "Automatic Secret Keys From Reciprocal MIMO Wireless Channels: Measurement and Analysis" Information Forensics and Security, IEEE Transactions on , vol.5, no.3, pp.381-392.

[86] Renna F., Bloch M.R., Laurenti N. 2011. "Semi-blind key-agreement over MIMO fading channels", IEEE Transactions on Communications, vol.61,no.2, pp.620-627.

[87] Jorswieck E.A., Wolf, A., Engelmann, S.2013. "Secret key generation from reciprocal spatially correlated MIMO channels" in Globecom Workshops IEEE, pp.1245-1250.

[88] Engelmann S., Wolf A., Jorswieck E.A. 2014. "Precoding for secret key generation in multiple antenna channels with statistical channel state information", IEEE ICASSP, pp. 1592-1595.

[89] Tomasin S., Jorswieck E.2014. "Pilot-based secret key agreement for reciprocal correlated MIMOME block fading channels",in Globecom Workshops, pp.1343-1348.

[90] Chen K., Natarajan B.B., Shattil S. 2015. "Secret Key Generation Rate With Power Allocation in Relay-Based LTE-A Networks" in Information Forensics and Security, IEEE Transactions on , vol.10, no.11, pp.2424-2434.

[91] NIST.2001. "Statistical test suite for random and pseudorandom number generators for cryptographic applications" 2001.

[92] Tucker D.C., Tagliarini G.A. 2009. "Prototyping with GNU radio and the USRP - where to begin," IEEE SOUTHEASTCON, pp.50-54.

[93] Kleider J.E., Steenhoek C., Morris D., Lai H.-Q., Zannetti B., Chin T., Xiaoli M., Hamilton B. 2010. "Achieving MIMO performance with single-antenna radios", IEEE Military Communications Conference, pp. 814-819.

[94] Xiaolong L., Weihong H., Yousefizadeh H., Qureshi A. 2008. "A case study of a MIMO SDR implementation," IEEE Military Communications Conference, pp.1-7.

[95] Niculescu D. 2010. "Finding MIMO", IEEE Int'l. Symp. on Wireless Pervasive Computing (ISWPC), pp.267-272.

[96] Miller R., Jain S., Trappe W. 2008. "Radio teaming: Establishing communication when communication is not possible," IEEE Int'l. Conf. on Mobile Ad Hoc and Sensor Systems, pp.365-370.

[97] Marwanto A., Sarijari M.A., Norsheila F., Yusof S.K.S., Rashid R.A. 2009. "Experimental study of OFDM implementation utilizing GNU Radio and USRP - SDR", IEEE Malaysia Int'l. Conf. on Communications (MICC), pp.132-135.

[98] Tichy M., Ulovec K. 2012. "OFDM system implementation using a USRP unit for testing purposes," Int'l. Conf. Radioelektronika, pp.1-4.

[99] Fedra Z., Dimitrijevic B., Milosevic N., Stosovic S., Nikolic Z. 2011. "Low computing complexity frame synchronization for OFDM communication", Telecommunications Forum (TELFOR), pp.7-10.

[100] Wang H., Jouini W., Nafkha A., Palicot J., Cardoso L.S., Debbah M., 2010. "Blind standard identification with bandwidth shape and GI recognition using USRP platforms and SDR4all tools", Proc. of the Int'l. Conf. on Cognitive Radio Oriented Wireless Networks & Communications (CROWNCOM), pp.1-5.

[101] Pierrot A. J., Chou R. A., Bloch M.R. 2013. "Experimental Aspects of Secret-Key Generation in Indoor Wireless Environments", IEEE Workshop on Signal Processing Advances in Wireless Communications.

[102] Interdigital Technology Corporation, Alexander Reznik vd. US8238551 B2, Generation of perfectly secret keys in wireless communication networks.

[103] Interdigital Patent Holdings, Inc., Alexander Reznik, Joseph S. Levy, Yogendra C. Shah, Suhas Mathur, US20100131751, WO2010006035A2, WO2010006035A3, Support of physical layer security in wireless local area networks.

[104] Celeno Communications (Israel) Ltd., WO2012114233 A3, Phy-level wireless security.

[105] LG Electronics Inc., EP20,120,168,280, Ko, W. ve Moon, S., MIMO Precoding in a QAM system.

[106] Marvell World Trade Ltd., Melzer, E., Li, Y.N., Erell, A. ve Yellin, D., Precoding codebooks for MIMO communication systems, US Patent 8,391,392.

[107] Qualcomm Incorporated, Bhattad, K., Gaal, P., Gorokhov, A.Y. ve Montojo, J., "Feedback for supporting SU-MIMO and MU-MIMO operation in wireless communication", US Patent App. 13/011,595.

[108] Celeno Communications (Israel) Ltd., Shapira, N. ve Rozen, G., Method of secure WLAN communication, US Patent 7,656,965 .

[109] LG Electronics Inc., Hwang, D.S. and Kim, I.M., “Method and apparatus for secure data transmission”, US Patent App. 13/801,663.

[110] Mediatek Singapore Pte. Ltd., Lan, P.C., Low, T.P. ve Moon, J., Precoding-Codebook-Based Secure Uplink in LTE, US Patent App. 14/460,599.

[111] Broadcom Corporation, Kliger, A., “Beamforming precoding matrix using non-uniform angles quantization”, US Patent App. 13/346,170.

[112] FİNTEK FİNANSAL TEKNOLOJİ HİZMETLERİ ANONİM ŞİRKETİ, İLKER ARABACI TR20100004447T WO2008TR00129 20081112, Video konferans ile bankacılık işlemleri yapabilen bir cihaz ve buna ilişkin bir metot.

[113] FORD OTOMOTİV SANAYİ ANONİM ŞİRKETİ, TR20060003644 20060713, Bir güvenlik sistemi.

[114] US8879496 Beamforming codeword exchange between base stations, Nov 2014.

[115] WO2016157510A1, A communication system and A transmitter, October 2016.

[116] US20080137551 OFDMA with adaptive subcarrier-cluster configuration and selective loading, June 2008.

[117] Gökceli S.,Uslu M., Kurt G.K., Özbek B., Alakoca H., Durmaz M.A.2015. ’Implementation of Pre-FFT Beamforming in MIMO-OFDM’,9th International Conference on Electrical and Electronics Engineering (ELECO),Bursa.

[118] Uslu M., Tuğrel H.B., Kurt G.K., Özbek B. 2016. ’Yazılım Tabanlı Radyolarda Karşılıklı Kanal Özelliğinin İncelenmesi’, 24. Sinyal İşleme ve İletişim Uygulamaları (SİU2016), Zonguldak.

[119] Özdogan Ö., Özbek B., Kurt G.K. 2016. ’Güvenli çoklu kullanıcılı MISO sistemlerde eşik değerine dayalı kullanıcı seçim performansı’, 24. Sinyal İşleme ve İletişim Uygulamaları (SİU2016), Zonguldak.

[120] Özbek B., Özdogan Ö., Kurt G.K. 2016. ’Secure Multiuser MISO Communication Systems with Quantized Feedback’, 27th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), ispanya.

[121] Zhongding L., Chin F. P. S. 2004. "Post and pre-FFT beamforming in an OFDM system," IEEE 59th Vehicular Technology Conference, vol1, pp:39-43.

[122] Özbek B. Le Ruyet D. 2014. ’Feedback Strategies for Wireless Communication’, Springer-Verlag New York.

[123] National Instruments, http://www.ni.com.

[124] Yan Y.-H., Letaief K.B., Cao Z. 2004. 'MIMO/OFDM with adaptive interleaved beamforming and power allocation for high-capacity wireless access,' IEEE 59th Vehicular Technology Conference, vol4, pp:1906-1910.

[125] Achoura N., Bouallegue R. 2008. "Multi-user detection for MIMO-OFDM system using joint adaptive Beamforming", 3rd International Conference on Information and Communication Technologies: From Theory to Applications, pp:1-5.

[126] Elnoubi S., Abdallah W. 2012. "Minimum bit error rate (MBER) pre-FFT beamforming for OFDM communication systems", Japan-Egypt Conference on Electronics, Communications and Computers (JEC-ECC), pp:127-132.

[127] Jeon S.S., Wang Y., Qian Y., Itoh T. 2001. "Mixing of Technologies for Adaptive Beamforming Implementation," 31st European Microwave Conference, pp:1-4,

[128] Rahman M. M. , Baidoo-Williams H. E. , Mudumbai R. ,Dasgupta S.2012. "Fully wireless implementation of distributed beamforming on a software-defined radio platform", ACM/IEEE 11th International Conference on Information Processing in Sensor Networks (IPSN), pp:305-315.

[129] Quitin F., Madhow U., Rahman M.M.U., Mudumbai R. 2012. "Demonstrating distributed transmit beamforming with software-defined radios," IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), pp:1-3.

[130] Matsuoka H., Shoki H.2003. "Comparison of pre-FFT and post-FFT processing adaptive arrays for OFDM systems in the presence of co-channel interference," 14th IEEE Proceedings on Personal, Indoor and Mobile Radio Communications, vol2, pp:1603-1607.

[131] Ping'an L., Qin S., Zhao F. 2006. "Comparison of pre-FFT and post-FFT beamforming in wireless LANs," IET International Conference on Wireless, Mobile and Multimedia Networks, pp:1-4.

[132] Heakle M. S., Mangoud M. A., Elnoubi S. 2007. "LMS Beamforming Using Pre and Post-FFT Processing for OFDM Communication Systems," National Radio Science Conference, pp:1-7.

[133] Ping'an L., Zhaofengfei.2006. "A Novel Pre-FFT Beamforming for an OFDM System with an Antenna Array in WLAN", International Conference on Wireless Communications, Networking and Mobile Computing, pp:1-4.

[134] Hong Y. J. 2011. "Vigorous Study on Pre-FFT Smart Antennas in OFDM," Eighth International Conference on Information Technology: New Generations (ITNG), pp:131-134.

[135] Lei M., Zhang P., Harada H., Wakana H. 2004. "LMS adaptive beamforming based on pre-FFT combining for ultra high-data-rate OFDM system," IEEE 60th Vehicular Technology Conference, vol5, pp:3664-3668.

[136] Shenghai L., Suili F., Wu Y. 2007. "A Beamspace-based Pre-FFT Beam-forming Algorithm for OFDM Systems with Antenna Array," International Symposium on Microwave, Antenna, Propagation and EMC Technologies for Wireless Communications, pp:490-495.

[137] Fan L.Y., He C., Che X.L. 2005. "Pre-FFT adaptive beamformer based on RLS for OFDM systems," Antennas and Propagation Society International Symposium, vol3A, pp:291-294.

[138] Modulation Error Ratio (MER) and Error Vector Magnitude (EVM), http://www.ni.com/white-paper/3652/en/, 2014.

[139] Guillaud M., Slock D.T.M., Knopp R. 2005. "A practical method for wireless channel reciprocity exploitation through relative calibration," Proceedings of the Eighth International Symposium on Signal Processing and Its Applications, vol1, pp:403-406.

[140] Gao Q., Qin F., Sun S. 2010. "Utilization of channel reciprocity in advanced MIMO system," 5th International ICST Conference on Communications and Networking in China (CHINACOM), pp:1-5.

[141] Wilson R.,Tse D., Scholtz R.A. 2007. "Channel Identification: Secret Sharing Using Reciprocity in Ultrawideband Channels", IEEE Transactions on Information Forensics and Security, vol2, pp:364-375.

[142] Wallace J.W., Chen C., Jensen M.A. 2009. "Key generation exploiting MIMO channel evolution: Algorithms and theoretical limits," 3rd European Conference on Antennas and Propagation, pp:1449-1503.

[143] Wallace, J.W., Sharma R.K.2010. "Automatic Secret Keys From Reciprocal MIMO Wireless Channels: Measurement and Analysis," IEEE Transactions on Information Forensics and Security, vol5, pp:381-392.

[144] Hershey J.E., Hassan A.A., Yarlagadda R. 1995. "Unconventional cryptographic keying variable management," IEEE Transactions on Communications, vol43, pp:3-6.

[145] Hassan A. A., Stark W.,Hershey E., John E.,Chennakeshu S.1996. "Cryptographic key agreement for mobile radio" Digital Signal Processing, vol6, pp:207-212.

[146] Koorapaty H., Hassan A.A., Chennakeshu S. 2000. "Secure information transmission for mobile radio," IEEE Communications Letters, vol4, pp:52-55.

[147] Li Z., Li X., Wenyaun R., Miller T. 2006. "Securing wireless systems via lower layer enforcements," Proceedings of the 5th ACM workshop on Wireless security, pp:33-42.

[148] Shi Z., Wang Q., Jin J., Jiang D., Liu G.2010. "Achievability of the channel reciprocity and its benefit in TDD system," 5th International ICST Conference on Communications and Networking in China (CHINACOM), pp:1-4.

[149] Ran J., Li L. 2011. "An adaptive method utilizing channel reciprocity in TDD-LTE system," IET International Conference on Communication Technology and Application, pp:896-900.

[150] Sun M., Liu Q., Liang W, Wessel B.L., Roche P.A., Mickle M., Sclabassi R.J. 2003." Application of the reciprocity theorem to volume conduction based data communication systems between implantable devices and computers" 25th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, vol4, pp:3352-3355.

[151] Shahin N., LaSorte N.J., Rajab S.A., Refai H.H.2013. 802.11g channel characterization utilizing labview and NI-USRP, IEEE International Instrumentation and Measurement Technology Conference (I2MTC), pp:753-756.

[152] Hugl K., Kalliola K., Laurila J.,2002. "Spatial reciprocity of uplink and downlink radio channels in FDD systems," Proc. COST 273 Technical Document TD (02), vol:66, p:7.

[153] Promsuvana N., Uthansakul P. 2008. Feasibility of adaptive 4x4 MIMO system using channel reciprocity in FDD mode, 14th Asia-Pacific Conference on Communications, pp:1-5.

[154] Han Y., Ni J., Gaoke D.2010. "The potential approaches to achieve channel reciprocity in FDD system with frequency correction algorithms," 5th International ICST Conference on Communications and Networking in China (CHINACOM), pp:1-5.

[155] Haile S. "Investigation of channel reciprocity for OFDM TDD systems," University of Waterloo, 2009.

[156] Guey J.C., Larsson L.D. 2004. "Modeling and evaluation of MIMO systems exploiting channel reciprocity in TDD mode," IEEE 60th Vehicular Technology Conference, vol6, pp:4265-4269.

[157] Gao Q., Qin F., Sun S. 2010. "Utilization of channel reciprocity in advanced MIMO system", 5th International ICST Conference on Communications and Networking in China (CHINACOM), pp:1-5.

[158] Dias A.R., Bateman, D., Gosse K.2004. "Impact of RF front-end impairments and mobility on channel reciprocity for closed-loop multiple antenna techniques," 15th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, vol2, pp:1434-1438.

[159] Guey J-C.,Larsson, L.D. 2004. "Modeling and evaluation of MIMO systems exploiting channel reciprocity in TDD mode," IEEE 60th Vehicular Technology Conference, vol6, pp:4265-4269.

[160] Liu Z.-J.,Sun D.-C., Wang, J.-L., Yi K.-C. 2013. "Impact and compensation of I/Q imbalance on channel reciprocity of time-division-duplexing multiple-input multiple-output systems," IET Communications, vol7, pp:663-672.

[161] Promsuvana N., Uthansakul P. 2008. "Feasibility of adaptive 4x4 MIMO system using channel reciprocity in FDD mode," 14th Asia-Pacific Conference on Communications, pp:1-5.

[162] Gao Q., Qin F., Sun S. 2010. "Utilization of channel reciprocity in advanced MIMO system," 5th International ICST Conference on Communications and Networking in China (CHINACOM), pp:1-5.

[163] Han Y., Ni J., Du G. 2010. "The potential approaches to achieve channel reciprocity in FDD system with frequency correction algorithms," 5th International ICST Conference on Communications and Networking in China (CHINACOM, pp:1-5.

[164] Ran J., Li L., 2011. "An adaptive method utilizing channel reciprocity in TDD-LTE system," IET International Conference on Communication Technology and Application, pp:896-900.

[165] Kim J., Yoon Y.K. 2009. "Correlation analysis of MIMO subchannels in LOS environments," 11th International Conference on Advanced Communication Technology, vol1, pp:335-337.

[166] Chan C.2010. "Secret key establishment using wireless channels as common randomness in time-variant MIMO systems," Brigham Young University.

[167] Taha H., Alsusa E. 2015. "A MIMO Precoding Based Physical Layer Security Technique for Key Exchange Encryption," IEEE 81st Vehicular Technology Conference (VTC Spring), pp:1-5.

[168] Kaltenberger F., Jiang H., Guillaud M., Knopp R.2010. Relative channel reciprocity calibration in MIMO/TDD systems, Future Network and Mobile Summit, pp:1-10.

[169] Kaltenberger F., Guillaud M., Oestges C., Czink N., Bandemer B., Castiglione P., Kountouris M., Gesbert D., Knopp R., Sacristan-Murga D. and others. 2009." Exploitation of reciprocity in measured MIMO channels," COST 2100, 9th Management Committee Meeting, TD (09), vol950.

[170] Qiu R. C., Zhou C.,Zhang J.Q.,Guo N. 2007. "Channel reciprocity and time-reversed propagation for ultra-wideband communications," IEEE Antennas and Propagation Society International Symposium, pp:29-32.

[171] Eugene C. H. Y., Sakaguchi K., Araki K.2004. "Experimental and analytical investigation of MIMO channel capacity in an indoor line-of-sight (LOS) environment," 15th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, vol1, pp:295-300.

[172] Fernandez O. Domingo M., Torres R.P. 2005. "Empirical analysis of the correlation of MIMO channels in indoor scenarios at 2 GHz," IEEE Proceedings - Communications, vol152, pp:82-88.

[173] Sakaguchi K., and Hai-Yeow-Eugene, CHUA and Araki, Kiyomichi .2005. "MIMO channel capacity in an indoor line-of-sight (LOS) environment," IEICE transactions on communications, vol88, pp:3010-3019.

[174] Plass S., Dammann A., Richter G., Bossert M.2008. "Channel correlation properties in OFDM by using time-varying cyclic delay diversity," Journal of Communications, vol3, pp:19-26

[175] Jeong W.H., Kim J.S., Kim K.-S., Jung M.-W., Kim J.-H., Yoon Y.K. 2012." Correlation analysis of MIMO channel measurement parameters under 781MHz environment," 42nd European Microwave Conference (EuMC), pp:866-870.

[176] Wu X.,Peng Y., Hu, C., Zhao H., Shu Lei 2013. "A secret key generation method based on CSI in OFDM-FDD system," IEEE Globecom Workshops, pp:1297-1302.

[177] Yasukawa S., Iwai H., Sasaoka H. 2008. "Adaptive key generation in secret key agreement scheme based on the channel characteristics in ofdm," International Symposium on Information Theory and Its Applications.

[178] Hamida S.T.B.,Pierrot J.B., Castelluccia C. 2009. "An Adaptive Quantization Algorithm for Secret Key Generation Using Radio Channel Measurements," NTMS, pp:1-5.

[179] Zhang J., Woods R., Marshall A., Duong T.Q. 2015. IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp:1727-1731.

[180] Wallace J. W., Sharma R. K., 2010. "Automatic secret keys from reciprocal MIMO wireless channels: Measurement and analysis," IEEE Transactions on Information Forensics and Security, vol5, pp:381-392.

[181] Mathur S., Trappe W., Mandayam N., Ye C., Reznik A. 2008. "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," Proceedings of the 14th ACM international conference on Mobile computing and networking, pp:128-139.

[182] Hamida S.T.B., Pierrot, J.-B., Castelluccia C. 2010. "Empirical analysis of UWB channel characteristics for secret key generation in indoor environments," IEEE 21st International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC), pp:1984-1989.

[183] Liu H., Wang Y., Jie Y., Chen Y. 2013. "Fast and practical secret key extraction by exploiting channel response," Proceedings IEEE INFOCOM, pp:3048-3056.

[184] Ambekar A., Hassan M., Schotten H. D.2012. "Improving channel reciprocity for effective key management systems," International Symposium on Signals, Systems, and Electronics (ISSSE), pp:1-4.

[185] Castelluccia C., Tmar-Ben, Hamida S., Pierrot J-B., Benoit D.,Uguen B.2012. "On the security of UWB secret key generation methods against deterministic channel prediction attacks", Vehicular Technology Conference (VTC).

[186] Zeng K. 2015. "Physical layer key generation in wireless networks: challenges and opportunities", IEEE Communications Magazine, vol53, pp:33-39.

[187] Primak S.,Liu K., Wang X. 2014. "Secret key generation using physical channels with imperfect csi", IEEE 80th Vehicular Technology Conference (VTC Fall), pp:1-5.

[188] Zhang J., Marshall A., Woods R., Duong T. Q. 2014. "Secure key generation from OFDM subcarriers' channel responses," Globecom Workshops (GC Wkshps), pp:1302-1307.

TÜBİTAK
PROJE ÖZET BİLGİ FORMU

Proje Yürütücüsü:	Yrd. Doç. Dr. BERNA ÖZBEK
Proje No:	114E626
Proje Başlığı:	Zaman-Uzamsal İmzaya Dayalı Güvenli Çok-Girişli Çok-Çıkışlı Kablosuz Haberleşme Sistemi
Proje Türü:	1005 - Yeni Fikirler ve Ürünler
Proje Süresi:	18
Araştırmacılar:	GÜNEŞ ZEYNEP KARABULUT KURT
Danışmanlar:	
Projenin Yürütüldüğü Kuruluş ve Adresi:	İZMİR YÜKSEK TEKNOLOJİ ENS. MÜHENDİSLİK F. ELEKTRİK-ELEKTRONİK MÜH
Projenin Başlangıç ve Bitiş Tarihleri:	01/04/2015 - 01/10/2016
Onaylanan Bütçe:	129030.0
Harcanan Bütçe:	60378.8
Öz:	Kablosuz haberleşme sistemlerinde kullanılan kanalın açık bir ortam olması ve iletilen işaretin vericinin kapsama alanı içerisinde kalan her alıcının erişimi dahilinde olması, gizli dinleme türü, pasif güvenlik ihlallerine olanak sağlamaktadır. Bu ihlallere karşı günümüzde kullanılan güvenlik sistemleri, şifreleme çözümlerine dayanmaktadır. Fakat söz konusu verilerin gönderici tarafta şifrelenmesi ve alıcı tarafta şifre çözme işleminin yapılması gecikmeyi daha da arttıracaktır. Bu sebeple şifreleme yöntemleri, gecikmeye duyarlı gerçek zamanlı iletişim sistemlerinde güvenlik seviyesini yüksek tutacak düzeyde yapılamamaktadır. Ayrıca şifrelemede oluşan hesaplama karmaşıklığı, taşınabilir cihazların pil kullanım ömrünü azaltmaktadır. Veri iletimindeki güvenlik seviyesinin arttırılması önemli bir problemdir ve halen çözüm beklemektedir. Yeni nesil haberleşme sistemlerinde kullanılan çoklu antenli yapılar ile uzayda iletim seçiciliği sağlanarak güvenlik çözümleri geliştirilebilir. Bu projede, çoklu girişli çoklu çıkışlı (MIMO) dikgen frekans bölmeli çoğullama (OFDM) tabanlı kablosuz haberleşme sistemlerinde uzay, zaman ve frekanstaki seçicilik özelliklerini kullanarak kanal imzaları hem iç mekan ve hem de dış mekan uygulamaları için çıkartılmıştır. Yetkili kulllanıcıya iletilecek verinin güvenliğinin sağlanması ve gizli alıcılar tarafından sezinlenme olasılığı azaltmak için kablosuz kanalın faz ve genlik bilgisi nicemlenmiş ve hüzmeleme yöntemi gerçekleştirilmiştir. Projemiz iki iş paketi olarak planlanmış ve her bir iş paketinin hedeflerine ulaşılmıştır. İlk iş paketinde MIMO-OFDM tabanlı kablosuz haberleşme sistemleri için verimli fiziksel katman güvenlik yöntemleri tasarlanmıştır. Geliştirilen kod kitapçığı, kullanıcı seçimi ve önkodlama yöntemleri ile MIMO-OFDM tekniğinin uzay, zaman ve frekans seçicilik avantajı kullanılarak, gizli dinleyici saldırıları mevcut tekniklere göre daha verimli olarak engellenmiş ve güvenlik kapasitesi arttırılmıştır. İkinci iş paketinde ise MIMO-OFDM sistemi için fiziksel katman güvenliğinin yazılım tabanlı radyo düğümleri ile gerçeklenmesi yapılmıştır. Karşılıklı kanal özelliği ile şifreleme için kullanılacak anahtarların uzunluğu belirlenmiş ve güvenlik anahtarı çıkarımı için anahtar hata oranının teorik analizi elde edilmiştir.
Anahtar Kelimeler:	Fiziksel katman güvenliği;MIMO-OFDM;Yazılım tabanlı radyo
Fikri Ürün Bildirim Formu Sunuldu Mu?:	Evet
Projeden Yapılan Yayınlar:	1- Implementation of pre-FFT beamforming in MIMO-OFDM (Bildiri - Uluslararası Bildiri - Sözlü Sunum), 2- Yazılım Tabanlı Radyolarda Karşılıklı Kanal Özelliğinin İncelenmesi (Bildiri - Ulusal Bildiri - Sözlü Sunum), 3- Güvenli çoklu kullanıcılı MISO sistemlerde eşik değerine dayalı kullanıcı seçim performansı' (Bildiri - Ulusal Bildiri - Sözlü Sunum), 4- Secure Multiuser MISO Communication Systems with Quantized Feedback (Bildiri - Uluslararası Bildiri - Sözlü Sunum),