ÖZET

MESAFE TABANLI ALT TAŞIYICI MODÜLASYONU VE RF BOZULMASI PİLOT KODLAMA SİSTEMİ VE YÖNTEMİ

Buluş, veri korumasını arttırmak için mesafe tabanlı alt taşıyıcı modülasyonu ve RF bozulması pilot kodlamasını kullanan güvenli havadan karaya (A2G) iletişime yönelik bir sistem ve yöntem ile ilgilidir. Sistem karşılıklı kanal karakteristikleri ve benzersiz alt taşıyıcı sönümleme manipülasyonunu kullanarak, düşman girişimi varlığında bile, bir hava ileticisi (örneğin UAV - İnsansız Hava Aracı veya Yüksek İrtifa Platformu) ve bir kara alıcısı arasındaki meşru iletişim bağlantılarının güvenli kalmasını sağlamaktadır. Gürültü etkilerinin hafifletilmesi için, sistem gelişmiş gürültü ortalaması alma için çoklu giriş çoklu çıkış (MIMO) teknolojisini içermektedir, böylece daha hassas anahtar üretimi ve güvenilir iletim sağlamaktadır. Önerilen yöntem etkili, sağlam ve güvenilir bir iletişim çerçevesini sağlamakta, böylece fiziksel-katman zafiyetlerinden faydalanılmasını önlemektedir.

İSTEMLER

1. Buluş, aşağıdaki adımları içeren, mesafe tabanlı bir alt taşıyıcı modülasyonu ve RF bozulması pilot kodlama yöntemi ile ilgilidir:

— B düğümünden A düğümüne bir yer-uydu bağı sinyalinin alınması,

— A düğümü tarafından karaya olan mesafenin ölçülmesi,

— A düğümü tarafından, alınan yer-uydu bağı sinyaline dayanarak B düğümünün RF bozulmalarının ölçülmesi,

— ölçülen mesafeye dayanarak A düğümü tarafından alt taşıyıcıların modüle edilmesi, burada alt taşıyıcılardan bazıları sadece belirli bir mesafede sönümlemektedir,

— alt taşıyıcı pilotlarının, ölçülen RF bozulmalarına dayanarak sönümlemeyen alt taşıyıcılar için benzersiz bir takımuydu diyagramına modüle edilmesi,

— belirli bir modülasyon için ideal takımuydu diyagramı ve RF bozulması tabanlı modülasyonun takımuydu noktaları arasındaki mesafeleri içeren bir kod tablosunun hem A düğümü hem de B düğümünde oluşturulması,

— bir uydu-yer bağı sinyalinin B düğümü tarafından alınması, sönümlemeyen alt taşıyıcıların demodüle edilmesi ve zaman, frekans veya uzamsal çeşitliliği içeren çeşitlilik yaklaşımlarını kullanarak gürültü etkilerinin ortalamasının alınması,

— demodüle edilmiş alınan noktalar ve ideal takımuydu noktaları arasındaki mesafenin ölçülmesi ve bunun oluşturulan kod tablosundaki mesafeler ile karşılaştırılması,

— mesafe farkı bir spesifik eşiğin altındaysa bir “0” bitinin atanması ve değilse bir “1” bitinin atanması

— mesafe farkı tüm noktalar spesifik eşiğin altındaysa düğümün yetkilendirilmesi ve

— A düğümü ve B düğümü arasında güvenli bir bağlantının kurulması ve önerilen kod tablosuna dayanarak verilerin iletilmesi.

2. Gürültü etkilerinin ortalamasının alınması için kullanılan çeşitlilik yaklaşımının zaman çeşitliliğini içerdiği, İstem 1’e göre yöntem.

3. Gürültü etkilerinin ortalamasının alınması için kullanılan çeşitlilik yaklaşımının frekans çeşitliliğini içerdiği, İstem 1'e göre yöntem.

4. Gürültü etkilerinin ortalamasının alınması için kullanılan çeşitlilik yaklaşımının uzamsal çeşitliliği içerdiği, İstem 1'e göre yöntem.

5. Mesafe farklarının belirlenmesi için spesifik eşiğin önceden tanımlandığı ve iletişim ortamına göre konfigüre edilebildiği, İstem 1'e göre yöntem.

TARİFNAME

MESAFE TABANLI ALT TAŞIYICI MODÜLASYONU VE RF BOZULMASI PİLOT KODLAMA SİSTEMİ VE YÖNTEMİ

Teknik Alan:

Buluş, bir hava ileticisi ve bir kara alıcısı arasında veri korumasına odaklanan, mesafe tabanlı bir alt taşıyıcı modülasyonu ve RF bozulması pilot kodlama sistemi ve yöntemi ile ilgilidir.

Tekniğin Bilinen Durumu:

Havadan karaya (A2G) bağlantılar, sinyalleri havadayken yakalayan havadaki gizli dinleyiciler ve meşru kullanıcıların yakınında bulunmaktan faydalanan karadaki saldırganlar dahil olmak üzere düşmanlara karşı zafiyete sahiptir. Kablosuz iletişimin, bu ağlarda görüş hattı ile birleştirilmiş yayın yapısı bu tehditleri arttırmaktadır. Geleneksel kriptografik teknikler, hesaplama karmaşıklıkları ve gecikmelerinden dolayı uygun değilken, mevcut fiziksel katman güvenliği önlemleri dinamik düşman senaryolarına uyarlanabilirlikten yoksundur.

Kablosuz iletişimin güvence altına alınması uzun süredir var olan bir zorluktur ve A2G bağlantılarının güvenliğini arttırmak için çeşitli teknikler önerilmiştir. Alt taşıyıcı indeksleme, RF parmak izi alma ve derin öğrenme tabanlı yöntemler dahil olmak üzere bazı yaklaşımlar alana önemli katkılarda bulunmuştur. Ancak bu çözümler, özellikle de FANET'ler gibi dinamik ve kaynak bakımından kısıtlı ortamlarda önemli sınırlandırmalardan muzdariptir. Aşağıda bu mevcut yöntemler ve eksikliklerinin bir özeti verilmiştir:

1.Alt Taşıyıcı İndeks Seçimli OFDM (OFDM-SIS):

Bu teknik, veri iletimi için alt taşıyıcıları dinamik olarak seçerek öngörülemezlik yaratmakta ve gizli dinleme girişimlerini zorlaştırmaktadır. Bununla birlikte, meşru alıcıları seçim modelinden haberdar etmek için önemli bir sinyalleme ek yükü gerektirmektedir ve bu da karmaşıklığı arttırmaktadır. Üstelik gelişmiş hesaplama kaynaklarına sahip düşmanlar zaman içinde alt taşıyıcı modellerini yeniden oluşturarak güvenliği tehlikeye atabilmektedir [1].

2.Alt Taşıyıcı İndeks Modülasyonu (SIM):

SIM, aktif alt taşıyıcıların indekslerine bilgi kodlayarak spektral verimliliği arttırmaktadır. Güvenliği arttırırken, teknik alt taşıyıcı indeksinin ve sembol verilerinin aynı anda çözülmesinin hataya açık hale geldiği çok yollu sönümlenme ortamlarında zorlanmaktadır. Yüksek kod çözme karmaşıklığı, FANET'ler gibi yüksek mobiliteli sistemlerde uygulanabilirliği daha da sınırlandırmaktadır [2].

3.İndeks Modülasyonu Tabanlı Rastgele Alt Taşıyıcı Seçimi:

Bu yaklaşım, alt taşıyıcı aktivasyonuna rastgelelik getirerek düşman müdahalesini zorlaştırmaktadır. Bununla birlikte, alt taşıyıcılar arasında eşit olmayan güç dağılımına yol açarak sistem verimliliğini azaltabilmektedir. Ayrıca zayıf kanal koşulları meşru alıcılar için kod çözme performansını düşürmektedir [3].

4.Cihaz Kimlik Doğrulaması için RF Parmak İzi Alma:

RF parmak izi alma, cihazların kimliğini doğrulamak için osilatör kayması ve amplifikatörün doğrusal olmaması gibi donanıma özgü kusurlardan yararlanmaktadır. Kontrollü ortamlarda etkili olan bu yaklaşım, parmak izlerini değiştirebilen sıcaklık ve hareketlilik gibi çevresel faktörlere karşı hassastır. Parmak izlerinin çıkarılması ve doğrulanması için gereken hesaplama yükü de özellikle kısıtlı sistemlerde gerçek zamanlı uygulanabilirliği sınırlamaktadır [4].

5.Derin Öğrenme Tabanlı RF Parmak İzi Alma:

Derin öğrenme modelleri, cihaz sınıflandırması ve kimlik doğrulaması için RF sinyallerinden karmaşık özellikler çıkarmaktadır. Bu teknikler gürültüye karşı oldukça dayanıklıdır ve karmaşık sinyal modellerine uyarlanabilmektedir. Bununla birlikte, dronlar gibi hafif veya mobil sistemler için pratik olmayan kapsamlı eğitim veri kümeleri ve önemli hesaplama kaynakları gerektirirler. Ayrıca dinamik ortamlara uyum sağlamak için modellerin yeniden eğitilmesi ek karmaşıklık getirmektedir [5].

6.Geçici Sinyal Analizi ile RF Parmak İzi Alma:

Bu teknik, bir RF sinyalinin başlangıç aşaması sırasında cihaza özgü benzersiz özellikleri tanımlamaktadır. Bu geçici sinyallerin kopyalanması zordur ve kimlik doğrulama için sağlam bir temel sunmaktadır. Ancak bu sinyallerin kısa ömürlü olması, özellikle gürültülü ortamlarda doğru bir şekilde yakalanmalarını zorlaştırmaktadır. Yüksek çözünürlüklü

donanıma olan bağımlılık, bu yaklaşımın pratik sistemlerde ölçeklenebilirliğini daha da sınırlandırmaktadır [6].

7.Kararlı Durum Sinyal Özelliklerini Kullanarak RF Parmak İzi Alma:

Bu yöntem, faz gürültüsü veya spektral şekil gibi sabit durum RF özelliklerini analiz ederek, uzun oturumlar boyunca tutarlı cihaz tanımlaması sağlamaktadır. Ancak bu özellikler çevresel gürültüye karşı daha savunmasızdır ve doğruluğu sağlamak için karmaşık sinyal işleme gerektirmektedir. Bu tür işlemlerin hesaplama maliyeti de dinamik veya kaynak kısıtlı sistemlerde kullanımını sınırlandırmaktadır [7].

Bu teknikler alanı ilerletmiş olsa da önemli zorluklarla karşı karşıyadır. Alt taşıyıcı tabanlı yöntemler sinyalleşme ek yükü, kod çözme karmaşıklığı ve çok yollu ortamlarda etkinliğin azalmasından muzdariptir. RF parmak izi yöntemleri, umut verici olmasına rağmen, çevresel değişikliklere karşı hassastır, yüksek hesaplama kaynakları gerektirmektedir ve FANET'lerdeki gerçek zamanlı uygulamalar için ölçeklenebilirlikten yoksundur.

Sonuç olarak, havadan karaya iletişim için güvenli ve verimli bir yöntem sağlayarak belirtilen dezavantajları gideren, verileri düşmanca girişimlere karşı koruyabilen, gürültü etkilerini en aza indiren ve mesafe tabanlı alt taşıyıcı modülasyonu ve pilot kodlama yoluyla güvenilir anahtar üretimi sağlayan yeni bir sisteme ihtiyaç vardır.

Referanslar:

[1]. J. M. Hamamreh, & H. Arslan, "OFDM-Subcarrier Index Selection for Enhancing Security and Reliability of 5G URLLC Services," *IEEE Access*, cilt. 5, s. 25863-25875, 2017.

[2]. M. Wen, vd., "Subcarrier Index Modulation for Future Wireless Networks: Principles, Applications, and Challenges," *IEEE Wireless Communications*, cilt. 27, no. 3, s. 118-125, 2020.

[3]. Y. Zhang, vd., "A Random Subcarrier-Selection Method Based on Index Modulation for Secure Wireless Communication," *Sensors*, cilt. 22, no. 7, s. 2676, 2022.

[4]. B. Danev, vd., "Physical-layer identification of RFID devices," *ACM Computing Surveys*, cilt. 45, no. 1, s. 1-29, 2012.

[5]. F. Restuccia, vd., "DeepRadioID: Real-Time Channel-Resilient Optimization of Deep Learning-Based Radio Fingerprinting Algorithms," *IEEE Transactions on Mobile Computing*, cilt. 18, no. 11, s. 2593-2608, 2019.

[6]. V. Brik, vd., “Wireless device identification with radiometric signatures,” *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking*, s. 116-127, 2008.

[7]. B. Danev, & S. Capkun, “Transient-based identification of wireless sensor nodes,” *Proceedings of the 8th ACM/IEEE International Conference on Information Processing in Sensor Networks*, s. 25-36, 2009.

Buluşun Açıklaması:

Bu buluş, Yüksek İrtifa Platformu (HAP) veya herhangi bir hava platformundan Karasal Ağa (TN) iletişimde, özellikle de gözetleme, afet müdahalesi ve IoT uygulamaları için giderek daha fazla kullanılan Uçan Ad-Hoc Ağlarında (FANET’ler) artan güvenlik sorunlarını ele almaktadır.

Buluş, afet kurtarma, gözetim ve IoT tabanlı araç sistemleri gibi uygulamalardaki kritik ihtiyaçları ele alarak FANET’lerdeki A2G bağlantılarının fiziksel katman güvenliğini arttırmak için çığır açan bir yaklaşım sunmaktadır. Buluş, kanala duyarlı mesafe modülasyonunu RF bozulmasına dayalı parmak izi ile birleştirerek hem havadan hem de karadan gelen tehditlere karşı sağlam bir koruma sağlamaktadır. Bu yenilikçi teknikler, ölçeklenebilir, düşük gecikmeli ve hesaplama açısından verimli bir güvenlik çözümü sunarak yüksek hareketlilik ve yakınlık tabanlı tehditlerle ilişkili temel zorlukların üstesinden gelmek için tasarlanmıştır. İletişim kanalının doğal fiziksel ve cihaza özgü özelliklerinden yararlanan buluş, geleneksel kriptografik yöntemlere olan ihtiyacı ortadan kaldırarak dronlar ve IoT cihazları gibi gerçek zamanlı ve kaynak kısıtlı ortamlar için idealdir.

FANET’lerde doğrudan uygulanmasının ötesinde, buluşun IQ dengesizliği gibi kontrollü RF bozulmalarını bir güvenlik mekanizması olarak kullanması, kablosuz iletişim güvenliğinde yeni bir paradigma ortaya koymaktadır. Bu yaklaşım, dinamik ve gürültülü ortamlarda sağlam bir uyumluluk sağlayarak güvenilirliği arttırmaktadır. Buluşun çok yönlülüğü, onu araçtan her şeye (V2X) iletişim, akıllı şebeke ağları ve yüksek irtifa platform sistemleri gibi diğer kritik alanlara da uygulanabilir kılmaktadır. A2G bağlantılarındaki güvenlik açıklarını ölçeklenebilmektedir ve verimli bir çerçeveyle ele alan bu buluş, yeni nesil kablosuz ağlarda güvenli, gerçek zamanlı iletişim için yeni bir ölçüt oluşturmakta ve gelişmekte olan 6G ve IoT özellikli sistemler için sağlam bir temel sağlamaktadır.

Bu buluş, sağlam koruma için fiziksel katman özelliklerinden yararlanan yeni bir çift katmanlı güvenlik mekanizması sunmaktadır. Hava düşmanlarına karşı, mesafe tabanlı bir alt taşıyıcı modülasyon tekniği, meşru kullanıcının tam konumuna bağlı olarak alt taşıyıcı etkinliğini dinamik olarak modüle etmektedir. Bu, sinyallerin yalnızca amaçlanan mesafede çözülebilir olmasını sağlayarak ara kesmeleri işe yaramaz hale getirmektedir. Kara tabanlı düşmanlar için, RF bozulmasına dayalı pilot modülasyonu, meşru alıcının IQ dengesizliği ve faz gürültüsü gibi doğal RF bozulmalarına dayanan benzersiz takımuydu tasarımlarına sahip pilotları kodlamaktadır. Bu parmak izleri yakındaki saldırganlar tarafından algılanamaz, böylece yalnızca meşru kullanıcının iletilen sinyali çözebilmesini sağlamaktadır.

Önerilen çözüm hafif, ölçeklenebilir ve FANET'lerin ve A2G ağlarının dinamik doğasıyla uyumludur. Geleneksel kriptografiye olan bağımlılığı ortadan kaldırarak, yeni nesil kablosuz sistemlere uyarlanmış gerçek zamanlı, hesaplama açısından verimli bir güvenlik çerçevesi sunmaktadır. Bu yaklaşım, mesafeye bağlı modülasyonu kullanıcıya özgü RF bozulma parmak izi ile birleştirerek A2G bağlantılarındaki kritik güvenlik açıklarını gidermektedir ve hem hava hem de kara tabanlı düşmanlara karşı sağlam koruma sağlamaktadır.

Buluş, FANET'lerde A2G iletişim bağlantılarının fiziksel katman güvenliğini arttırmak için sağlam, ölçeklenebilir ve hesaplama açısından verimli bir çözüm sağlamayı amaçlamaktadır. Kanala duyarlı mesafe modülasyonu ve RF bozulmasına dayalı parmak izini entegre ederek, dinamik, yüksek mobilite ve kaynak kısıtlı ortamlarda hava ve kara düşmanlarının oluşturduğu güvenlik açıklarını gidermektedir. Hesaplama karmaşıklığı ve gecikmeye neden olan geleneksel kriptografik yöntemlerin aksine, bu buluş gerçek zamanlı güvenlik sağlamak için doğal fiziksel katman özelliklerinden ve cihaza özgü bozulmalardan yararlanmaktadır. Çözüm, afet müdahalesi, askeri gözetim ve IoT tabanlı araç ağları gibi kritik uygulamaları güvence altına almak için tasarlanmıştır ve FANET'lerin benzersiz zorluklarına göre uyarlanmış güvenilir ve verimli bir güvenlik mekanizması sunmaktadır.

Bu buluş, özellikle FANET'ler gibi yüksek hareketlilik ve dinamik koşullarla karakterize edilen ortamlarda, merkezi olmayan ve düşmanca senaryolarda güvenli kablosuz iletişim elde etmenin bilimsel zorluğunu ele almaktadır. Geleneksel güvenlik çözümleri, genellikle hesaplama açısından pahalı, gecikmeye neden olan ve gerçek zamanlı, kaynak kısıtlı sistemler için pratik olmayan kriptografik yöntemlere dayanmaktadır. Üstelik kablosuz kanalların yayın

doğası, özellikle düşmanlar meşru kullanıcılarla ilişkili kanal koşullarından yararlandığında, onları doğal olarak gizli dinlemeye karşı savunmasız hale getirmektedir. Bu buluş, kanal karşılıklılığı ve RF bozulmaları gibi fiziksel katman özelliklerinden yararlanarak hafif ve uyarlanabilir bir güvenlik çerçevesi sunmaktadır. Paradigmayı geleneksel kriptografiden, FANET'lerin ve diğer yeni nesil kablosuz sistemlerin benzersiz gereksinimlerini karşılayan yenilikçi fiziksel katman güvenlik tekniklerine kaydırmaktadır.

Bu buluş, FANET'lerde A2G bağlantılarının güvenliğinin sağlanmasıyla ilgili kritik teknik zorlukları çözmektedir:

1. Gizli Dinlemeye Karşı Zafiyet: Geleneksel yöntemler, ortak kanal özellikleri ve korelasyon koşulları nedeniyle hava ve kara düşmanlarına karşı iletişimi güvence altına almakta zorlanmaktadır. Buluş, yalnızca meşru kullanıcılar tarafından erişilebilen alt taşıyıcıları modüle etmek için mesafeye bağlı sönümlemeyi kullanan ve ele geçirilen sinyalleri hava düşmanları için kullanılamaz hale getiren kanala duyarlı mesafe modülasyonunu tanıtmaktadır.
2. Yakınlık Tabanlı Tehditler: Meşru alıcıların yakınındaki kara düşmanları, örtüşen kanal özellikleri nedeniyle önemli riskler oluşturmaktadır. Buluş, yalnızca meşru kullanıcıların çözebileceği benzersiz, tekrarlanabilir parmak izleri oluşturmak için IQ dengesizliği gibi cihaza özgü kusurlardan yararlanarak RF bozulmasına dayalı parmak izi kullanarak buna karşı koymaktadır.
3. Ölçeklenebilirlik ve Gerçek Zamanlı Güvenlik: Mevcut kriptografik teknikler hesaplama açısından yoğundur ve yüksek mobiliteye sahip FANET'ler için uygun değildir. Önerilen çözüm, doğal fiziksel katman özelliklerinden yararlanarak kriptografik değişim ihtiyacını ortadan kaldırmaktadır, düşük gecikme süresi ve ölçeklenebilir güvenlik sağlamaktadır.
4. Çekişmeli Ortamlarda İletişim Güvenilirliği: Gürültü ve dinamik kanal koşulları sıklıkla genel performansını bozmaktadır. Bu buluş, MIMO tabanlı gürültü ortalamasını içermekte ve zorlu senaryolarda bile sağlam ve güvenli iletişimi sürdürmektedir.

Bu buluş, özellikle FANET'lerdeki A2G bağlantıları için güvenli kablosuz iletişimde son teknolojiyi ilerleten birkaç önemli yenilik getirmektedir. İlk olarak, kablosuz kanalların mesafeye bağlı sönümleme özelliklerinden yararlanan yeni bir yaklaşım olan kanala duyarlı mesafe modülasyonundan yararlanmaktadır. Alt taşıyıcıların meşru alıcılar için erişilebilir

kalırken düşmanlar için sönümlemeye karşı seçici olarak modüle edilmesini sağlayarak, buluş geleneksel kriptografik anahtar değişimlerine ihtiyaç duymadan sağlam bir fiziksel katman güvenlik mekanizması sağlamaktadır. Bu, kaynak kısıtlı ve yüksek hareket kabiliyetine sahip sistemlerde gerçek zamanlı iletişimin güvence altına alınmasında önemli bir sıçramayı temsil etmektedir.

İkinci olarak, buluş, IQ dengesizliği gibi cihaza özgü kusurları güvenilir güvenlik özelliklerine dönüştüren bir teknik olan RF bozulmasına dayalı parmak izini tanıtmaktadır. Buluş, bu bozulmaları düzeltmek yerine, bunları düşmanların kolayca kopyalayamayacağı benzersiz ve tekrarlanabilir parmak izleri oluşturmak için kullanmaktadır. Bu yaklaşım, önceden paylaşılan kriptografik anahtarlara olan bağımlılığı ortadan kaldırmaktadır ve hafif, ölçeklenebilir ve çevresel değişikliklere karşı dayanıklı yeni bir güvenlik katmanı eklemektedir. Bu yenilikler birlikte, afet kurtarma, gözetleme, askeri operasyonlar ve IoT tabanlı araç sistemleri gibi sektörlerde güvenli iletişim için yeni bir ölçüt oluşturmakta ve mevcut yöntemlerin etkili bir şekilde çözemediği zorlukları ele almaktadır.

Buluş, özellikle FANET'ler gibi yüksek mobiliteli sistemlerde kablosuz iletişim güvenliğinde mevcut çözümlerden ayıran çeşitli avantajlar ve benzersiz özellikler sunmaktadır. Temel avantajlar aşağıdakilerden oluşmaktadır:

1. Hafif ve Hesaplama Açısından Verimli Güvenlik: Önemli hesaplama ek yükü ve gecikme süresi getiren geleneksel kriptografik yöntemlerin aksine, buluş gerçek zamanlı, düşük gecikmeli güvenlik sağlamak için kanal karşılıklılığı ve RF bozulmaları gibi fiziksel katman özelliklerinden yararlanmaktadır. Bu sayede dronlar ve IoT cihazları gibi kaynak kısıtlaması olan ortamlar için son derece uygundur.
2. Hava ve Kara Düşmanlarına Karşı Sağlam Koruma: Buluş, belirli alt taşıyıcıların meşru kullanıcılar için etkili kalırken havadaki düşmanlar için erişilemez olmasını sağlamak için kanala duyarlı mesafe modülasyonu kullanarak A2G iletişim bağlantıları için kapsamlı koruma sunmaktadır. Bu seçici alt taşıyıcı sönümlemesi, özellikle yüksek mobilite ve son derece dinamik ortamlarda dinleme ve gizli dinleme riskini azaltmaktadır.
3. Cihaza Özel RF Bozulmalarından Yararlanma: Buluşun benzersiz bir unsuru, RF bozulmasına dayalı parmak izi kullanımıdır. Buluş, donanım bileşenlerindeki IQ dengesizliği gibi doğal kusurları düzeltmek yerine, bunları her cihaz için benzersiz,

tekrarlanabilir parmak izleri oluşturmak için kullanmaktadır. Bu, düşmanların çoğaltması veya manipüle etmesi zor olan yeni ve ölçeklenebilir bir güvenlik özelliği sağlamaktadır.

4. Uyarlanabilirlik ve Ölçeklenebilirlik: Buluş, gürültülü veya dengesiz ortamlarda bile iletişim güvenilirliğini arttırmak için gürültü ortalamasına yönelik MIMO tekniklerinden yararlanarak son derece uyarlanabilirdir. Çözüm, afet kurtarma ve askeri gözetimden araç ağlarına kadar farklı uygulamalar arasında iyi ölçeklenmektedir ve çeşitli senaryolarda kablosuz iletişimi güvence altına almak için çok yönlü ve verimli bir araç sunmaktadır.
5. Kriptografik Anahtar Değişimlerine İhtiyaç Duymama: Kablosuz kanalların fiziksel katman özelliklerine ve cihaza özgü parmak izlerine dayanan buluş, geleneksel kriptografik değişimlere olan ihtiyacı ortadan kaldırmaktadır. Bu, güvenlik sürecini basitleştirmektedir ve potansiyel saldırı yüzeyini azaltarak sistemi gerçek zamanlı uygulamalarda daha verimli ve güvenli hale getirmektedir.

Bu buluşun Çarpıcı Özelliği, kanala duyarlı mesafe modülasyonunu RF bozulmasına dayalı parmak izi ile birleştirme yeteneğinde yatmaktadır. Bu iki teknik birlikte hem hesaplama açısından verimli hem de yüksek mobilite ortamlarında bile gizli dinleme ve müdahaleyi önlemede oldukça etkili olan sağlam bir güvenlik mekanizması oluşturmaktadır.

- Kanala Duyarlı Mesafe Modülasyonu, alt taşıyıcıların seçici olarak sönümlemesini sağlayarak meşru kullanıcılar için güvenli hale getirirken havadan düşmanların erişimini engellemektedir, böylece karmaşık kriptografik protokollere gerek kalmadan güvenliği arttırmaktadır.
- RF Bozulmasına Dayalı Parmak İzi, cihaza özgü kusurları (IQ dengesizliği gibi) benzersiz ve güvenilir güvenlik özelliklerine dönüştürerek önceden paylaşılan anahtarlara ihtiyaç duymadan kimlik doğrulama ve güvenli iletişim sağlamaktadır.

Bu özellikler, mevcut kablosuz güvenlik teknolojilerinin önemli sınırlamalarını ele alan, ölçeklenebilir, gerçek zamanlı ve çok çeşitli yüksek mobiliteli, kaynak kısıtlı ortamlara uyarlanabilir bir güvenlik çözümü sunarak buluşu diğerlerinden ayırmaktadır.

Buluş konusu yöntemin yapısal ve karakteristik özellikleri ile tüm avantajları aşağıda verilen şekiller ve bu şekillere atıfta bulunularak yazılan detaylı açıklama sayesinde daha net anlaşılacağından değerlendirme bu şekiller ve ayrıntılı açıklama dikkate alınarak yapılmalıdır.

Şekillerin Açıklaması:

Buluşun özelliklerinin daha net anlaşılması ve takdir edilmesi için buluş, ekli şekillere atıfta bulunularak açıklanacaktır ancak bunun amacı buluşu bu belirli düzenlemelerle sınırlandırmak değildir. Aksine ekli istemler tarafından tanımlanan buluş alanına dahil edilebilecek tüm alternatifleri, değişiklikleri ve eşdeğerlikleri kapsaması amaçlanmaktadır. Gösterilen ayrıntıların sadece mevcut buluşun tercih edilen yapılandırmalarını tanımlamak amacıyla gösterildiği ve hem yöntemlerin şekillendirilmesi hem de buluşun kurallarının ve kavramsal özelliklerinin en uygun ve kolay anlaşılabilir şekilde tanımlanmasını sağlamak amacıyla sunulduğu anlaşılmalıdır. Bu şekillerde;

Şekil 1	Sistem modelinin ve problem formülasyonunun şematik bir görünümü.
Şekil 2	A ve B arasındaki bağlantının temsilinin bir görünümü.
Şekil 3	Önerilen teknik için örnek vakanın şematik bir görünümü.
Şekil 4A	A ve B için pilotların ayarlanmasının şematik bir görünümü.
Şekil 5A	A ve B için yapay olarak kaydırılmış pilotların ayarlanmasının şematik bir görünümü.
Şekil 6	Pilotun orijinal konumu ile yapay olarak bozulmuş versiyonu arasındaki mesafenin ölçülmesine ilişkin şematik bir görünüm.
Şekil 7	Pilotun orijinal konumu ile yapay olarak bozulmuş ve kanaldan geçirilmiş versiyonu arasındaki mesafenin ölçülmesine ilişkin şematik bir görünüm.
Şekil 8	Gürültünün takımuydu noktaları üzerindeki etkisinin şematik bir görünümü.
Şekil 9	MIMO kullanarak gürültü ortalamasının şematik bir görünümü.

Mevcut buluşun anlaşılmasına yardımcı olacak şekiller ekli resimde gösterildiği gibi numaralandırılmış ve aşağıda isimleriyle birlikte verilmiştir.

Referansların Açıklaması:

A. Verici

B. Alıcı

E_G . Kötü Amaçlı Düğüm

$H_{A2G.}$ Vericiden Alıcıya Kanal Karakteristiği

$H_{G2A.}$ Alıcıdan Vericiye Kanal Karakteristiği

$H_{A2E.}$ Vericiden drona Kanal Karakteristiği

d. Alıcıya Kötü Amaçlı Bir Düğüm

d_c Tutarlılık Mesafesi

Buluşun Ayrıntılı Açıklaması:

Şekil 1'de verilmiş önerilen sistem modelinde verici (A), verileri karadaki Meşru alıcıya (B) güvenli bir şekilde iletmeyi amaçlayan insansız hava aracı (UAV), Yüksek İrtifa Platformu (HAP) veya uydu gibi bir hava baz istasyonudur. Bu özel senaryo için hava platformu 20 km yükseklikte çalışan bir HAP olarak seçilmiştir. İletişim iki düşman tarafından tehdit edilmektedir: verici (A), meşru alıcı (B) arasına konumlandırılmış bir dron (E_A) ve meşru alıcıya (B) yakın bir konumda bulunan bir kötü amaçlı düğüm (E_G). Kötü amaçlı düğümün (E_G) meşru alıcıya (B) yakınlığı (d) tutarlılık mesafesi (d_c) dahilindedir, bu da hem verici (A) ile meşru alıcı (B) arasındaki meşru bağlantı hem de verici (A) ile kötü amaçlı düğüm (E_G) arasındaki düşmanca bağlantı için oldukça ilişkili veya aynı kanal özelliklerine neden olmaktadır. Bu durum önemli bir güvenlik sorunu yaratmaktadır, çünkü $d \leq dc$ olduğunda tipik olarak meşru kullanıcıları düşmanlardan ayıran fiziksel katman özellikleri ayırt edilemez hale gelmektedir.

Model, hava düşmanı olan dronun (E_A) ara konumunu kullanmak ve verici (A) ile meşru alıcı (B) arasındaki iletişimi kesmek için kendisini dinamik olarak konumlandırabileceğini vurgulamaktadır. Bu kurulum, Havadan Karaya (A2G) iletişimin hem hava hem de kara tabanlı tehditlere karşı güvence altına alınmasındaki kritik zorlukların altını çizmekte ve bu ortamlarda güvenli ve güvenilir veri iletimini sağlamak için sağlam ve yenilikçi çözümlere duyulan ihtiyacı vurgulamaktadır.

<u>Karşılıklı Kanal Tabanlı Anahtar Üretimi Başlatma:</u>

Önerilen senaryodaki birinci adım, alt taşıyıcı kazançlarındaki benzersiz kanal kaynaklı varyasyonlardan yararlanmaktadır. Tüm alt taşıyıcılar vericiden eşit güçle iletilmesine

rağmen, kanal bunların kazançlarını benzersiz bir şekilde değiştirerek farklı bir imza oluşturmaktadır. Bu özellikten faydalanmak için pilot sinyaller kanalın tutarlılık süresi içinde karşılıklı olarak değiştirilerek kanal tahmin edilmektedir. Tahmin edilen kanal bilgisi kullanılarak, seçilen alt taşıyıcıların konumları veya indeksleri belirlenmektedir ve bir bağıntı tablosu aracılığıyla anahtar bitleri oluşturmak için kullanılmaktadır. Daha da önemlisi, kanal A'dan B'ye ve B'den A'ya karşılıklı olduğu için, bağıntı tablosunun verici ve alıcı arasında açıkça paylaşılmasına gerek yoktur, bu da güvenliği korurken anahtar oluşturma sürecini basitleştirmektedir. Bu sürece ilişkin örnek Şekil 2'de verilmiş olup, burada $h_{B,i}$ verici (A) ve meşru alıcı (B) arasındaki belirli alt taşıyıcılara karşılık gelen kanal kazançlarını temsil etmektedir.

Tablo 1 A - B arasındaki bağlantı için örnek bir benzersiz bağıntı tablosu.

Alt bloklar	İndeksler	Anahtar Bitler
$[\lvert h_{\beta,1}\rvert\ 0\ 0\ \lvert h_{\beta,4}\rvert]$	{1, 4}	[0 0]
$[0\ \lvert h_{\beta,2}\rvert\ 0\ \lvert h_{\beta,4}\rvert]$	{2, 4}	[0 1]
$[\lvert h_{\beta,1}\rvert\ 0\ \lvert h_{\beta,3}\rvert\ 0]$	{1, 3}	[1 0]
$[0\ \lvert h_{\beta,2}\rvert\ \lvert h_{\beta,3}\rvert\ 0]$	{2, 3}	[1 1]

Mesafe Tabanlı Alt Taşıyıcı Sönümleme Manipülasyonu:

Sürecin ikinci adımında, aktif alt taşıyıcıların kazançları bağıntı tablosuna göre dikkatlice düzenlenmektedir ve geçerli bir anahtar bit çiftine karşılık gelmeyen alt taşıyıcıların meşru alıcı (B) için pasif kalması sağlanmaktadır. Bununla birlikte, aynı alt taşıyıcılar dron (EA) için aktif görünmekte olup, dron (EA) düşmanı yanılmaktadır. Bu tasarım, meşru bağlantı (A-B) ile düşman bağlantı (A- EA) arasındaki mesafe farkından yararlanarak, bu uzamsal ayrımın getirdiği benzersiz sönümleme özelliklerinden faydalanmaktadır. Özellikle meşru alıcı için pasif kalması gereken alt taşıyıcılar, meşru alıcının (B) tarafında sönümlenecek şekilde manipüle edilirken, düşman için hala aktif kalmaya devam etmektedir. Bu hedefli manipülasyon, dronun (EA) B'nin kodunu çözemediği alt taşıyıcılarda aktif bir iletim gözlemlemesini sağlayarak kasıtlı bir karışıklık yaratmakta ve sistemin güvenliğini arttırmaktadır. Burada alt taşıyıcılar pilotları değil, verileri tutmaktadır. Alım, bağıntı tablosu aracılığıyla yalnızca B'deki aktif alt taşıyıcılar tarafından gerçekleştirilmektedir. Hava düşmanı da veri çıkarımı için aktif alt taşıyıcı indekslerine ihtiyaç duyacağından, mesafe tabanlı modülasyon sayesinde kod çözme işlemi engellenecektir.

Bu tür bir iletim için örnek bir durum Şekil 3'te gösterilmektedir. Bu örnek durumda sistem, güvenliği sağlamak için alt taşıyıcı gücünün ve sönümleme özelliklerinin nasıl manipüle edildiğini göstermektedir. Yukarıda daha önce oluşturulan bağıntı tablosuna dayanarak, A ve B arasındaki belirli kanal için alt taşıyıcıların kazançları tanımlanmaktadır. Burada iletilmesi istenen anahtar bitler örnek olarak "00" verilmiştir. Bunu başarmak için, alt taşıyıcıların güçleri vericide tüm alt taşıyıcılar aktif olacak şekilde düzenlenmektedir. Bununla birlikte, benzersiz kanal özellikleri nedeniyle, meşru alıcı (B) için etkin olmaması amaçlanan alt taşıyıcılar, A-meşru alıcı (B) bağlantısının mesafesi boyunca sönümlemeye maruz kalacaktır. Eş zamanlı olarak, aynı alt taşıyıcılar A-dron (EA) kanalındaki farklı sönümleme davranışı nedeniyle dron (EA) için sönümlememektedir.

Bu süreç, A-B ve A-dron (EA) bağlantıları arasındaki mesafe farkını etkin bir şekilde kullanarak, meşru alıcının (B) amaçlanan aktif olmayan alt taşıyıcıları gözlemlerken, bunların düşman için tespit edilebilir kalmasını sağlamaktadır. Sonuç olarak, meşru alıcı (B) amaçlanan aktif olmayan alt taşıyıcılara dayanarak anahtar bitleri doğru bir şekilde çözebilirken, dron (EA) aktif alt taşıyıcıların ortaya çıkmasıyla yanlış yönlendirilmektedir. Bu örnek, mesafe tabanlı sönümleme manipülasyonunun düşmanların varlığında nasıl güvenli anahtar üretimi ve iletişim sağladığını göstermektedir.

Problem 1'i sonuçlandırmak için, yaklaşım kod tablosu tabanlı bir çerçevenin kullanılmasını öngörmektedir. Manipüle edilen alt taşıyıcılar üzerinde iletilen veriler kritik değildir ve rastgele verilerden ya da pilot sinyallerden oluşabilmektedir. Taşınan bu veri asıl gizli bilgiyi temsil etmediğinden, düşmanın buna erişim sağlaması kabul edilebilmektedir. Temel amaç, mesafe tabanlı alt taşıyıcı modülasyonundan yararlanılarak korunan gizli anahtarın düşman tarafından yeniden yapılandırılamamasını sağlamaktır. Bu, sistemin güvenliğinin fiziksel katman özelliklerine dayanmasını sağlayarak düşmanın iletilen veriler hakkındaki bilgisini anahtara ulaşmak için önemsiz hale getirmektedir.

A ve B için Karşılıklı Pilot Ayarı:

Üçüncü adım olarak sistem, meşru kullanıcının güvenliğini arttırmak için verici (A) ve alıcı (B) arasındaki benzersiz giriş/çıkış dengesizliğinden yararlanmaktadır. RF bozulmaları, özellikle faz içi (I) ve karesel (Q) bileşenler, iletilen sinyallere her bir verici-alıcı çiftine özgü

farklı özellikler katmaktadır. Bu farklılıklar tutarlı kalmaktadır ve bir düşman tarafından taklit edilemez, bu da kanal ayırt edici bir faktör olmadığında bile yeni bir güvenlik katmanı sağlamaktadır.

Bunu gerçekleştirmek için ilk olarak, Şekil 4'te gösterildiği üzere A ve B için pilot takımuydular karşılıklı bir şekilde $x_p \in x_{p1},x_{p2},x_{p3},x_{p4}$ olarak tanımlanmaktadır.

A ve B için karşılıklı yapay pilot ayarlama:

Bu, pilotların takımuydu noktalarının, Şekil 5'te gösterildiği üzere karşılıklı olarak takımuydu diyagramı üzerindeki spesifik bir konuma ayarlanmasıdır. Bu noktalar için gösterim $\hat{x}_p \in \{\hat{x}_{p1}, \hat{x}_{p2}, \hat{x}_{p3}, \hat{x}_{p4}\}$ şeklinde verilmiştir.

x_p ve $\hat{x}_p$ arasındaki Mesafenin Ölçülmesi:

Bu adımda, her bir takımuydu noktası çifti $x_{pi} - \widehat{x}_{pi}$ arasındaki mesafe ölçülmüş olup, burada $i \in \{1, 2, 3, 4\}$, ($d \in \{d_1,d_2,d_3,d_4\}$) şeklinde verilmiş ve Şekil 6'da gösterilmiştir.

Pilot tabanlı iletim:

$\hat{x}_p$ iletilmiş, kanaldan geçmiştir ve sinyalin bu versiyonu ($\tilde{x}_p \in \{\tilde{x}_{p1}, \tilde{x}_{p2}, \tilde{x}_{p3}, \tilde{x}_{p4}\}$) olarak gösterilmiştir. İletimden önce 0 veya 1'i iletmek için IQ parametreleri ile oynanmıştır. Daha sonra $d \in \{d_1, \tilde{d}_2, \tilde{d}_3, \tilde{d}_4\}$ olarak gösterilen her bir takımuydu noktası çifti $x_{pi} - \widetilde{x}_p$ arasındaki mesafeye bakılmıştır. Bu prosedür Şekil 7'de gösterilmiştir.

Bu tür bir takımuydu mesafe tabanlı yaklaşımdan faydalanarak, Tablo 1'de belirtildiği üzere alınan verilerin kodunu çözmek için bir bağıntı tablosu oluşturulmuştur. x_p ve $\tilde{x}_p$ elemanları arasındaki mesafe, x_p ve $\hat{x}_p$ elemanları arasındaki eşik mesafeden fazlaysa 0 olarak kodu çözülmektedir. x_p ve $\tilde{x}_p$ elemanları arasındaki mesafe, x_p ve $\hat{x}_p$ elemanları arasındaki eşik mesafeden azsa 1 olarak kodu çözülmektedir.

Tablo 2.Frekans ofseti mesafe tabanlı bağıntı tablosu

Bit Eşleyici	$d_1 - \hat{d}_1$	$d_2 - \hat{d}_2$	$d_3 - \hat{d}_3$	$d_4 - \hat{d}_4$
0000	$d_1 - \hat{d}_1 < 0$	$d_2 - \hat{d}_2 < 0$	$d_3 - \hat{d}_3 < 0$	$d_4 - \hat{d}_4 < 0$
0001	$d_1 - \hat{d}_1 < 0$	$d_2 - \hat{d}_2 < 0$	$d_3 - \hat{d}_3 < 0$	$d_4 - \hat{d}_4 > 0$
0010	$d_1 - \hat{d}_1 < 0$	$d_2 - \hat{d}_2 < 0$	$d_3 - \hat{d}_3 > 0$	$d_4 - \hat{d}_4 < 0$
0011	$d_1 - \hat{d}_1 < 0$	$d_2 - \hat{d}_2 < 0$	$d_3 - \hat{d}_3 > 0$	$d_4 - \hat{d}_4 > 0$
0100	$d_1 - \hat{d}_1 < 0$	$d_2 - \hat{d}_2 > 0$	$d_3 - \hat{d}_3 < 0$	$d_4 - \hat{d}_4 < 0$
0101	$d_1 - \hat{d}_1 < 0$	$d_2 - \hat{d}_2 > 0$	$d_3 - \hat{d}_3 < 0$	$d_4 - \hat{d}_4 > 0$
0110	$d_1 - \hat{d}_1 < 0$	$d_2 - \hat{d}_2 > 0$	$d_3 - \hat{d}_3 > 0$	$d_4 - \hat{d}_4 < 0$
0111	$d_1 - \hat{d}_1 < 0$	$d_2 - \hat{d}_2 > 0$	$d_3 - \hat{d}_3 > 0$	$d_4 - \hat{d}_4 > 0$
1000	$d_1 - \hat{d}_1 > 0$	$d_2 - \hat{d}_2 < 0$	$d_3 - \hat{d}_3 < 0$	$d_4 - \hat{d}_4 < 0$
1001	$d_1 - \hat{d}_1 > 0$	$d_2 - \hat{d}_2 < 0$	$d_3 - \hat{d}_3 < 0$	$d_4 - \hat{d}_4 > 0$
1010	$d_1 - \hat{d}_1 > 0$	$d_2 - \hat{d}_2 < 0$	$d_3 - \hat{d}_3 > 0$	$d_4 - \hat{d}_4 < 0$
1011	$d_1 - \hat{d}_1 > 0$	$d_2 - \hat{d}_2 < 0$	$d_3 - \hat{d}_3 > 0$	$d_4 - \hat{d}_4 > 0$
1100	$d_1 - \hat{d}_1 > 0$	$d_2 - \hat{d}_2 > 0$	$d_3 - \hat{d}_3 < 0$	$d_4 - \hat{d}_4 < 0$
1101	$d_1 - \hat{d}_1 > 0$	$d_2 - \hat{d}_2 > 0$	$d_3 - \hat{d}_3 < 0$	$d_4 - \hat{d}_4 > 0$
1110	$d_1 - \hat{d}_1 > 0$	$d_2 - \hat{d}_2 > 0$	$d_3 - \hat{d}_3 > 0$	$d_4 - \hat{d}_4 < 0$
1111	$d_1 - \hat{d}_1 > 0$	$d_2 - \hat{d}_2 > 0$	$d_3 - \hat{d}_3 > 0$	$d_4 - \hat{d}_4 > 0$

Anten alanında gürültü ortalaması alma:

Önerilen yöntem sadece gürültü etkisinin ihmal edildiği durumlarda geçerlidir ki bu mümkün değildir. Gürültünün etkisi takımuydu diyagramında çok büyük olacağı için, bu pilotlarda yapılan küçük değişiklikler Şekil 8'de gösterildiği gibi ihmal edilebilir olacaktır. Dolayısıyla bu küçük değişiklikleri görmek için gürültünün etkisinin ortalamasını almak gerekmiştir.

Geleneksel olarak bu gürültü ortalaması, ilk erişim için bir SSB bloğunda 4 OFDM sembolü kullanılarak elde edilmektedir. Bu tür bir ortalamanın ilk erişim için bir kez yapılması uygundur ancak önerilen teknik bu prosedürün her seferinde tekrarlanmasını gerektirmektedir, çünkü gürültü her örnek için değişmektedir, bu da önerilen tekniğin spektral olarak verimsiz olmasına neden olmaktadır. Bu sorunun üstesinden gelmek için, MIMO'yu tanıtarak zaman alanı yerine anten alanında ortalama alma işlemi yapılmıştır. Bu bağlamda, alıcıda 4 OFDM sembolü yerine 4 anten kullanılmış ve Şekil 9'da gösterildiği gibi alıcı çeşitliliğinden yararlanılmıştır. Bu yaklaşımda alıcıdaki anten sayısı arttıkça gürültü ortalamasının daha ince olacağı göz önünde bulundurulmalıdır.

Düşman, takımuyduda farklı bir IQ dengesizliğine sahip olduğu için, meşru kullanıcı için tanımlanan eşik değeri frekans ofsetiyle eşleşmeyecektir. Dolayısıyla düşman iletilen verileri çıkarmak için bağıntı tablosundan yararlanamayacaktır.

Önerilen teknik pilotları bir bağıntı tablosu ile birlikte kullanmaktadır. Bu, vericinin kaynak elemanlarında gerçek veri olmadığı anlamına gelmektedir. Dolayısıyla pilot sinyallerin faz ofsetleri ile yapay olarak oynasak bile, pilotlar alım tarafında zaten bilindiğinden, bu durum alıcının performansını etkilemeyecektir.

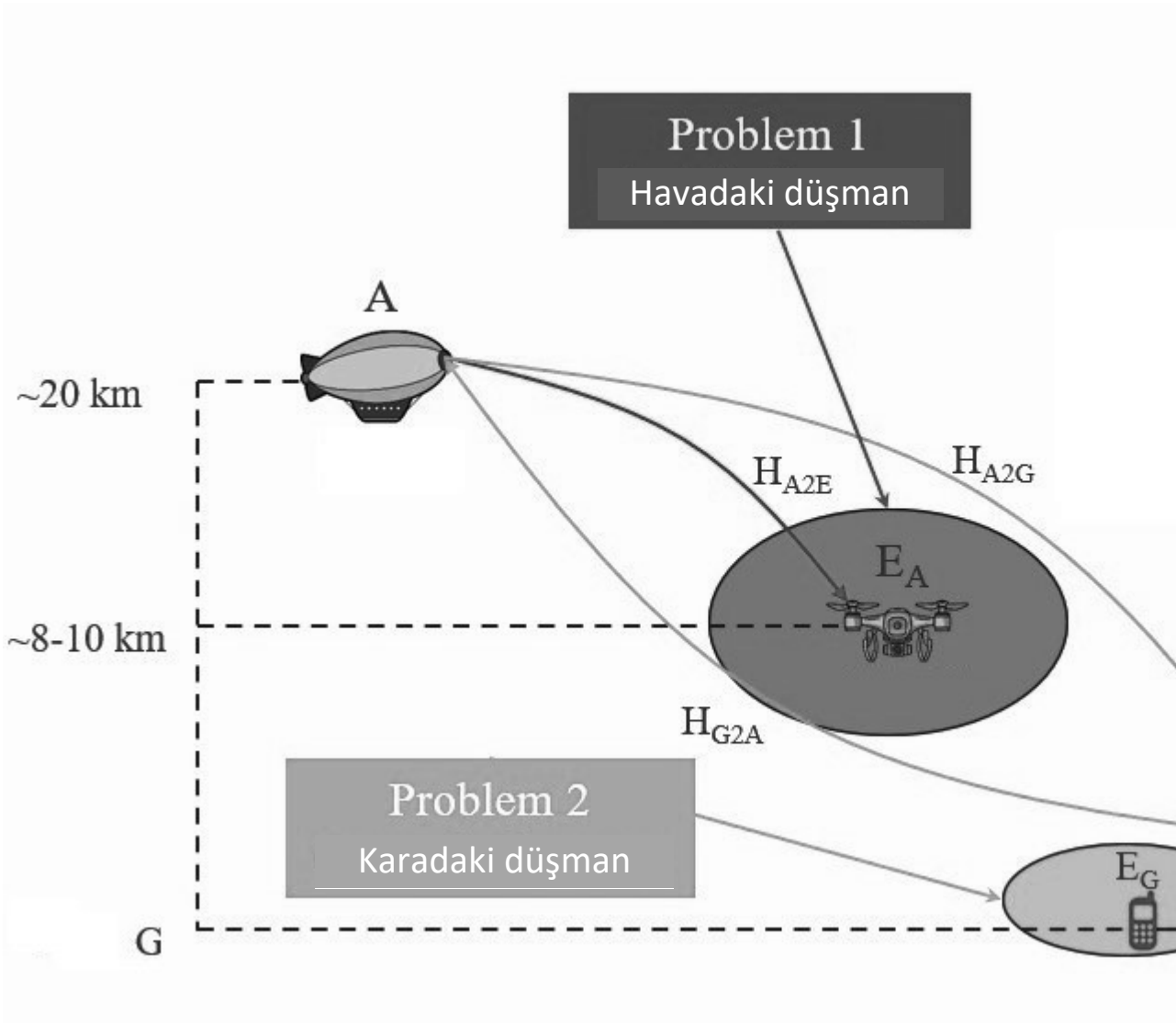
Önerilen yaklaşımın akış şeması aşağıda verilmiştir:

1. B düğümünden A düğümüne bir yer-uydu bağı sinyalinin alınması,
2. A düğümünün karaya olan mesafeyi ölçmesi,
3. A düğümünün alınan yer-uydu bağı sinyaline dayanarak B düğümünün RF bozulmalarını ölçmesi,
4. A düğümünün, ölçülen mesafeye dayanarak alt taşıyıcıları modüle etmesi, burada alt taşıyıcılardan bazıları sadece belirli bir mesafede sönümlemektedir,
5. Sönümlemeyen alt taşıyıcılar için, alt taşıyıcı pilotlarının ölçülen RF bozulmalarına dayanarak benzersiz takımuydu diyagramına modüle edilmesi,
6. Belirli bir modülasyon için ideal takımuydu diyagramı ve RF bozulması tabanlı modülasyonun takımuydu noktaları arasındaki mesafeleri içeren bir kod tablosunun hem A düğümü hem de B düğümünde oluşturulması,
7. B düğümünün uydu-yer bağı sinyalini alması, sönümlemeyen alt taşıyıcıları demodüle etmesi ve farklı çeşitlilik yaklaşımlarını (örneğin zaman, frekans, uzamsal) kullanarak gürültü etkisinin ortalamasını alması,
8. Demodüle edilmiş alınan noktalar ve ideal takımuydu noktaları arasındaki mesafenin ölçülmesi ve bunun oluşturulan kod tablosundaki mesafe ile karşılaştırılması,
9. Mesafe farkı belirli bir eşiğin altındaysa “0” bitinin verilmesi; değilse “1” bitinin verilmesi,
10. Mesafe farkı tüm noktalar için belirli bir eşiğin altındaysa düğümün yetkilendirilmesi,
11. A düğümü ile B düğümü arasında güvenli bağlantının kurulması ve önerilen kod tablosuna dayanarak verilerin iletilmesi.

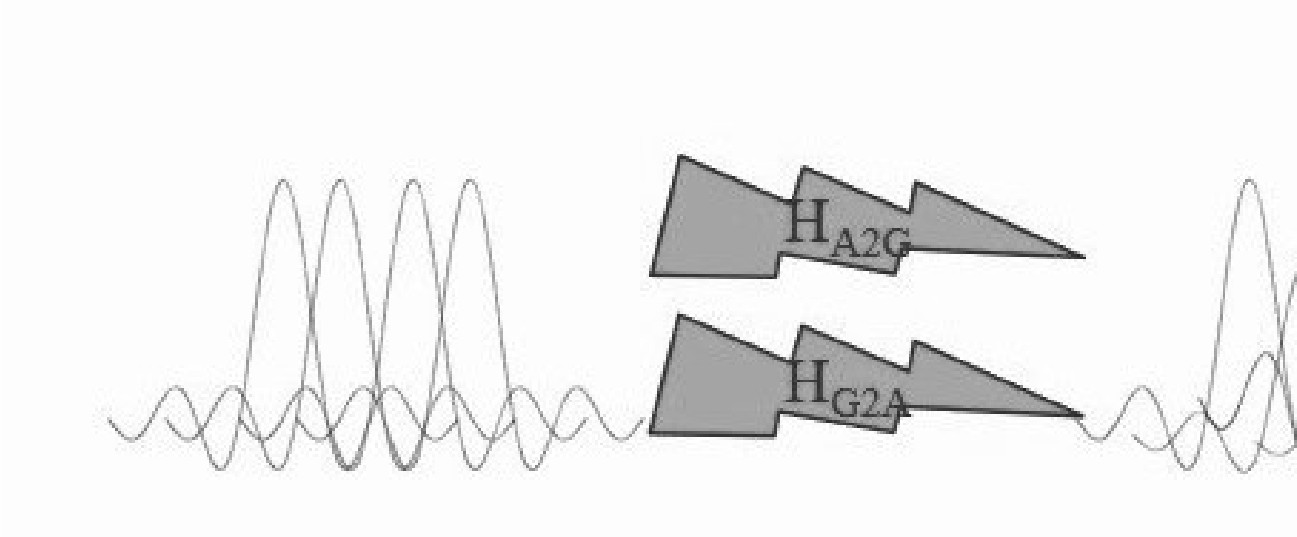
Mevcut teknolojinin çeşitli yapılandırmalarının yukarıdaki açıklamaları, sadece örnekleme ve açıklama amaçları için sunulmuştur. Bunların kapsamlı olması veya mevcut teknolojiyi açıklanan kesin formlarla sınırlandırması amaçlanmamıştır. Elbette yukarıdaki öğretiler dikkate alındığında birçok modifikasyon ve varyasyon mümkündür. Yapılandırmalar, mevcut

teknolojinin ilkeleri ve pratik uygulamalarının en iyi şekilde açıklanması amacıyla seçilmiş ve açıklanmıştır, böylece teknikte uzman kişiler, mevcut teknolojiyi ve özel kullanım amaçlarına uygun değişiklikler ile çeşitli yapılandırmaları en iyi şekilde kullanabilmektedir. Koşullar doğrultusunda sunulabilecek veya uygun hale getirilebilecek çeşitli atlamalar ve eşdeğerler ile değiştirmelerin öngörülebileceği göz önünde bulundurulmakla birlikte, bu tür değişiklikler mevcut teknolojinin özü veya istemlerinin kapsamından ayrılmaksızın yazılım veya uygulamayı kapsamalıdır.

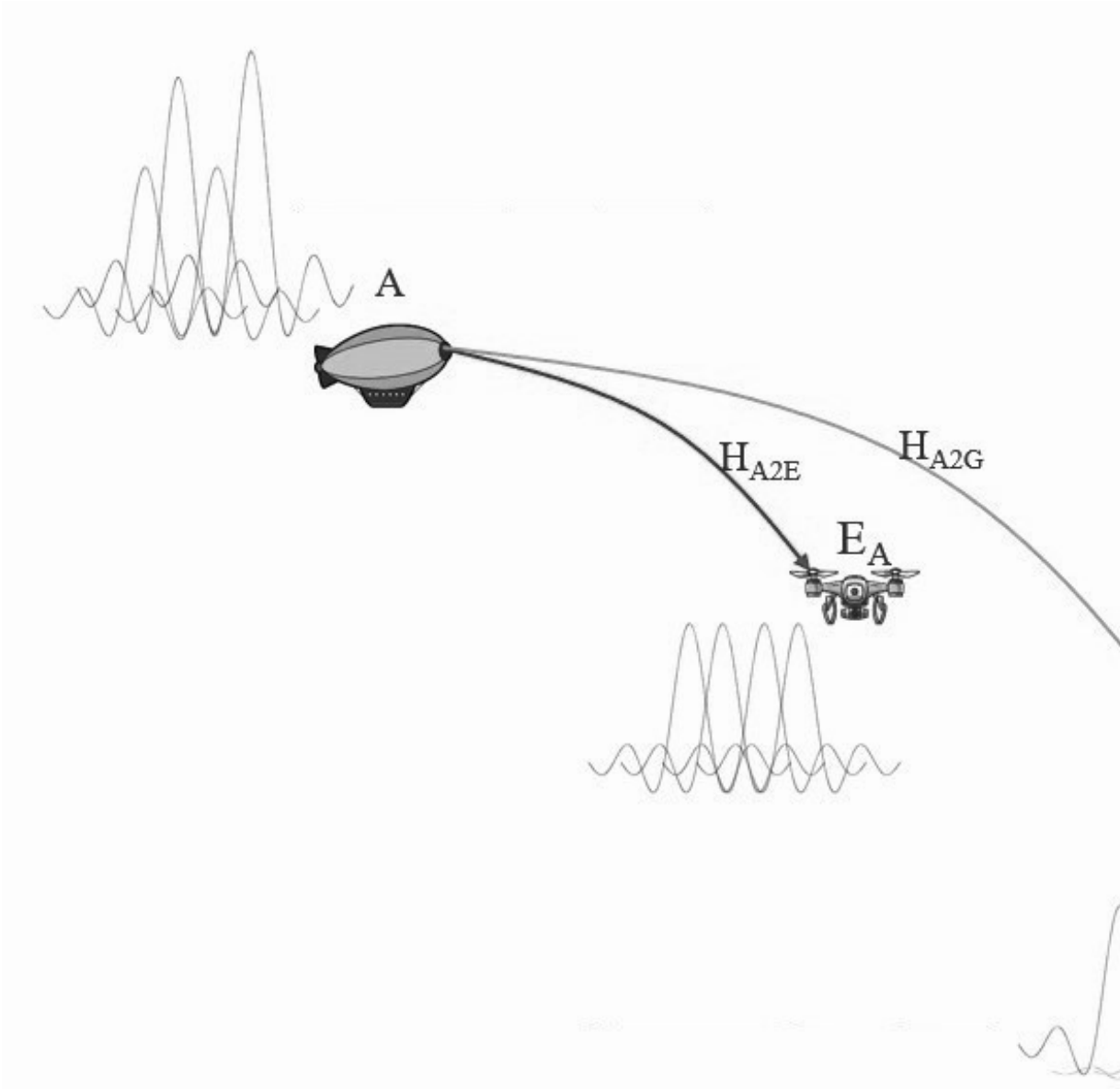
Herhangi bir çelişki olmadığı durumlarda, mevcut açıklamadaki yapılandırmalar ve bunların özellikleri birleştirilebilmektedir. Yukarıdaki açıklamalar sadece mevcut açıklamanın spesifik uygulamalarıdır ve koruma kapsamını sınırlama amacı taşımamaktadır. Mevcut açıklamanın teknik kapsamı dahilinde teknikte uzman bir kişi tarafından kolayca belirlenen herhangi bir varyasyon veya değiştirme, koruma kapsamına girecektir. Dolayısıyla mevcut açıklamanın koruma kapsamı istemler tarafından belirlenecektir.


Problem 1
Havadaki düşman
A
~20 km
H_{A2E}
H_{A2G}
E_A
~8-10 km
H_{G2A}
Problem 2
Karadaki düşman
E_G
G

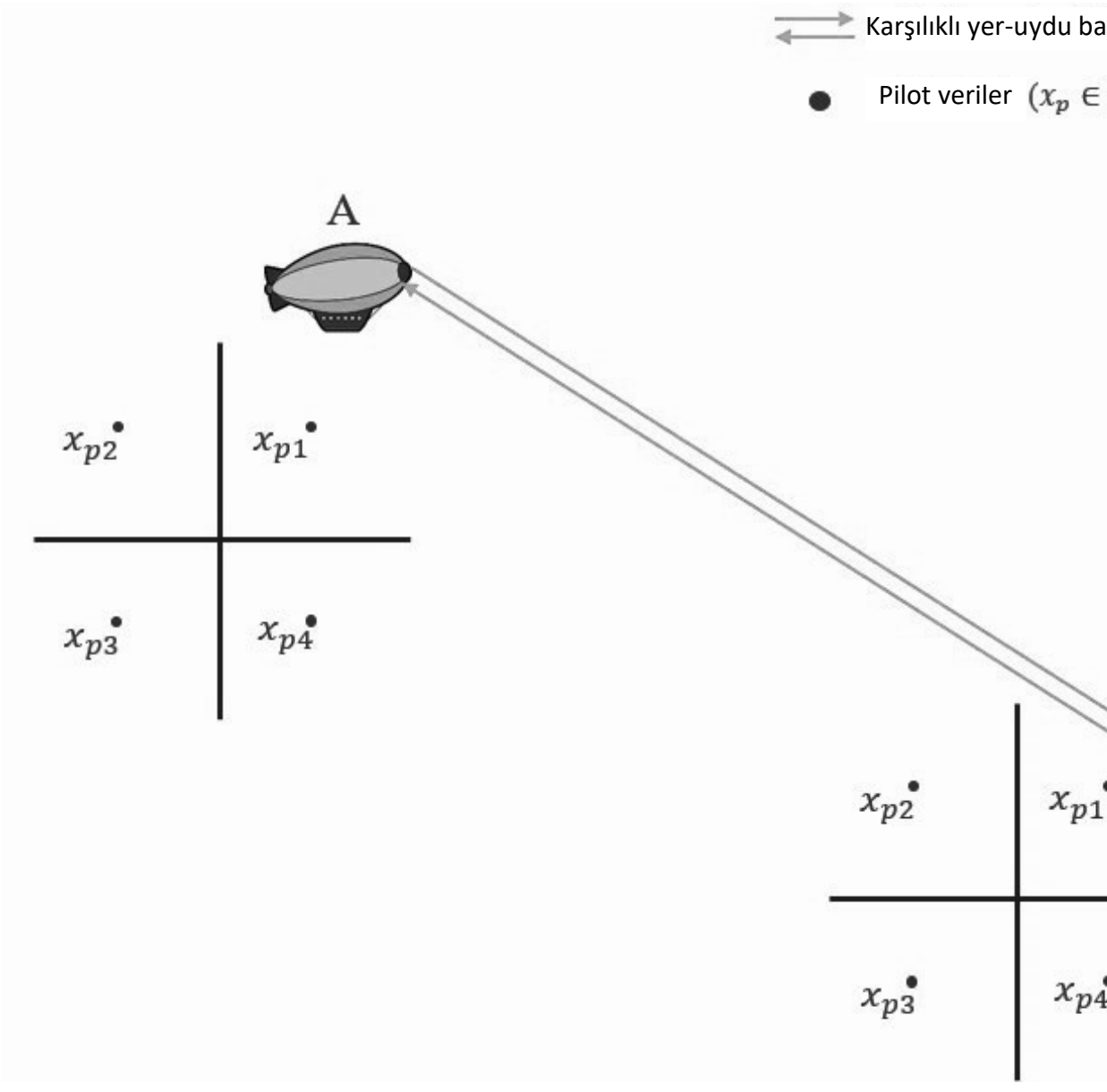
ŞEKİL 1



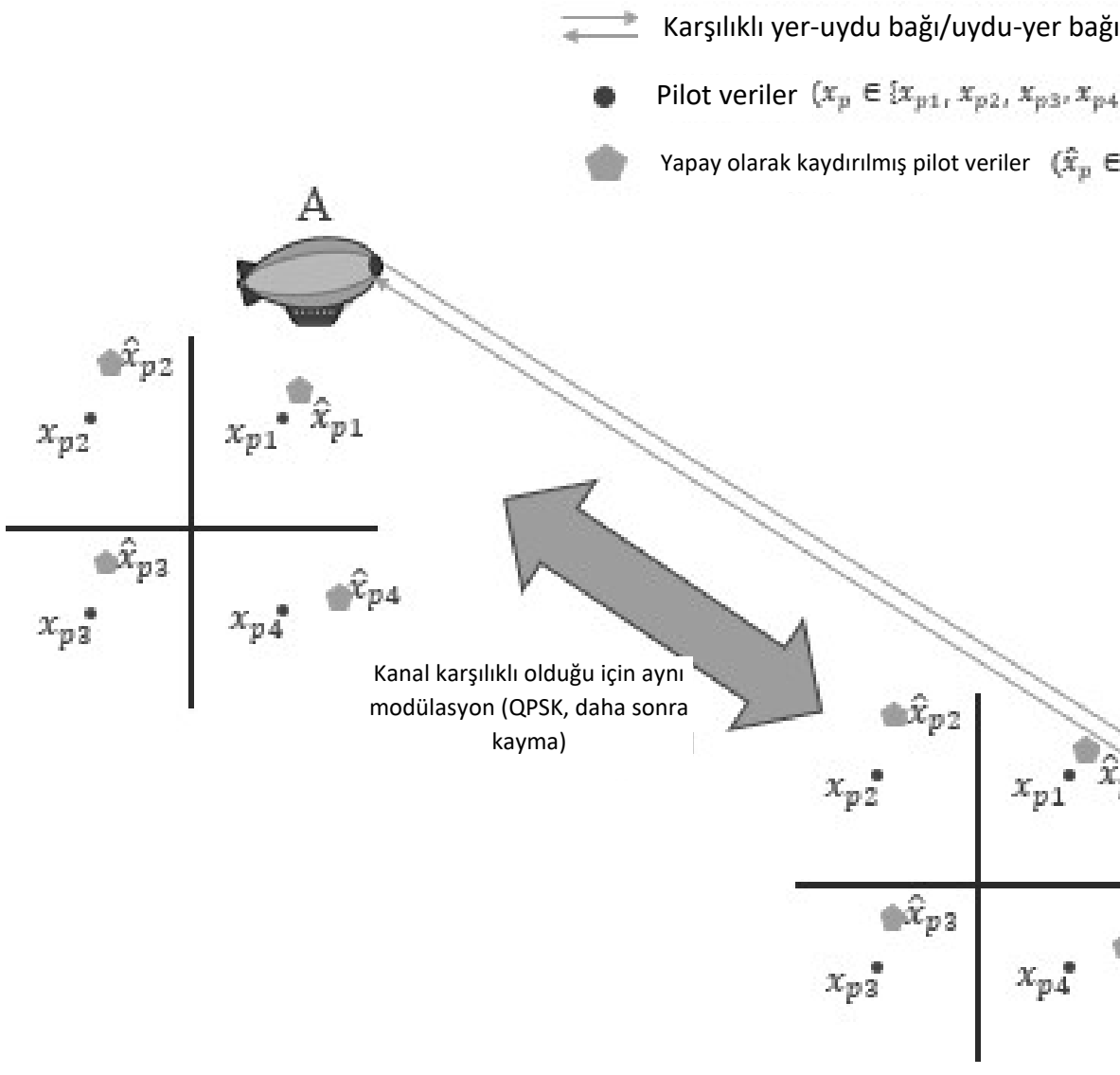
ŞEKİL 2



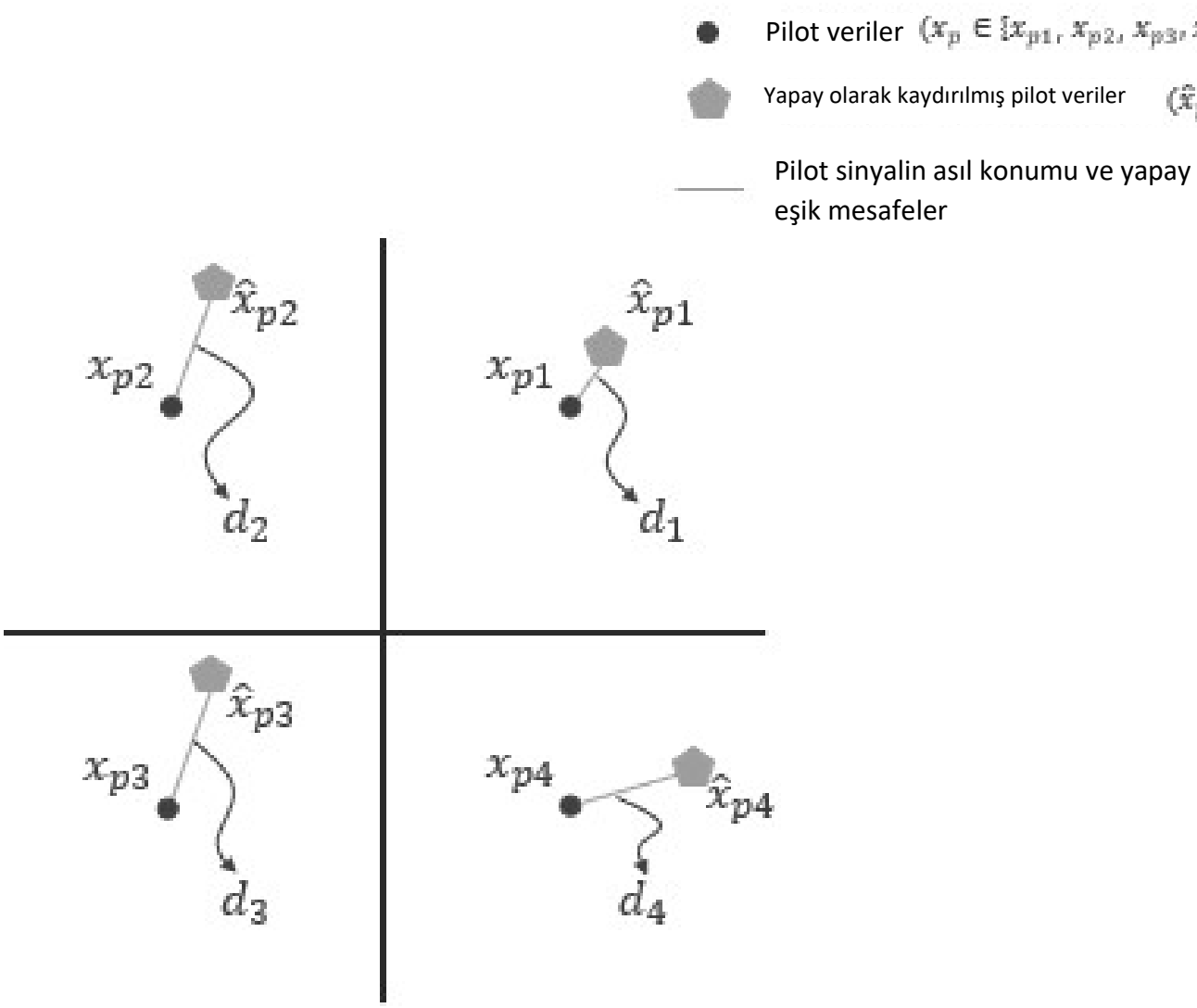
ŞEKİL 3


Karşılıklı yer-uydu ba
Pilot veriler $(x_p \in$
A
x_{p2}
x_{p1}
x_{p3}
x_{p4}
x_{p2}
x_{p1}
x_{p3}
x_{p4}

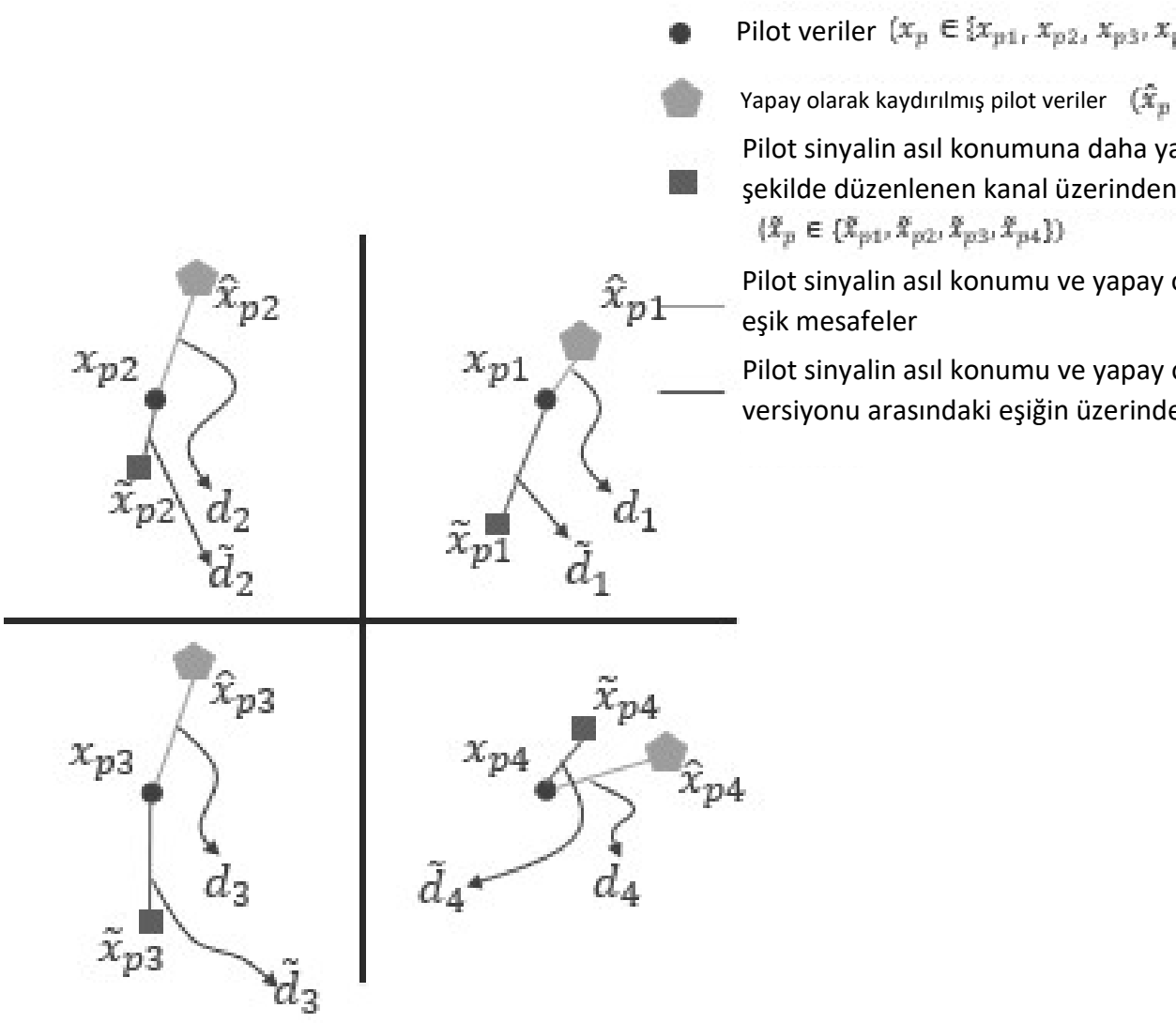
ŞEKİL 4


Karşılıklı yer-uydu bağı/uydu-yer bağı
Pilot veriler
Yapay olarak kaydırılmış pilot veriler
A
Kanal karşılıklı olduğu için aynı modülasyon (QPSK, daha sonra kayma)

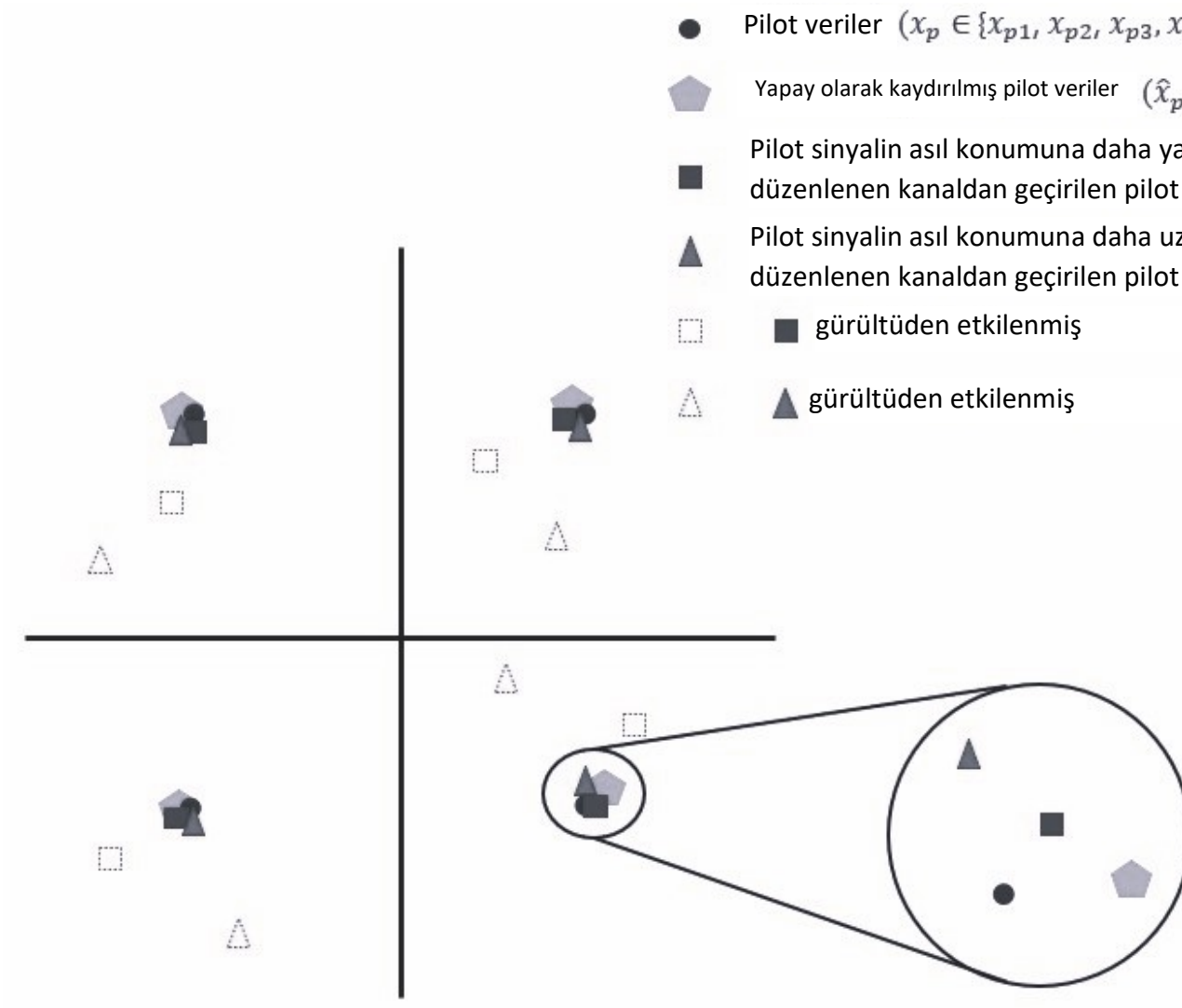
ŞEKİL 5


Pilot veriler
Yapay olarak kaydırılmış pilot veriler
Pilot sinyalin asıl konumu ve yapay
eşik mesafeler
$\hat{x}_{p2}$
x_{p2}
d_2
$\hat{x}_{p1}$
x_{p1}
d_1
$\hat{x}_{p3}$
x_{p3}
d_3
x_{p4}
$\hat{x}_{p4}$
d_4

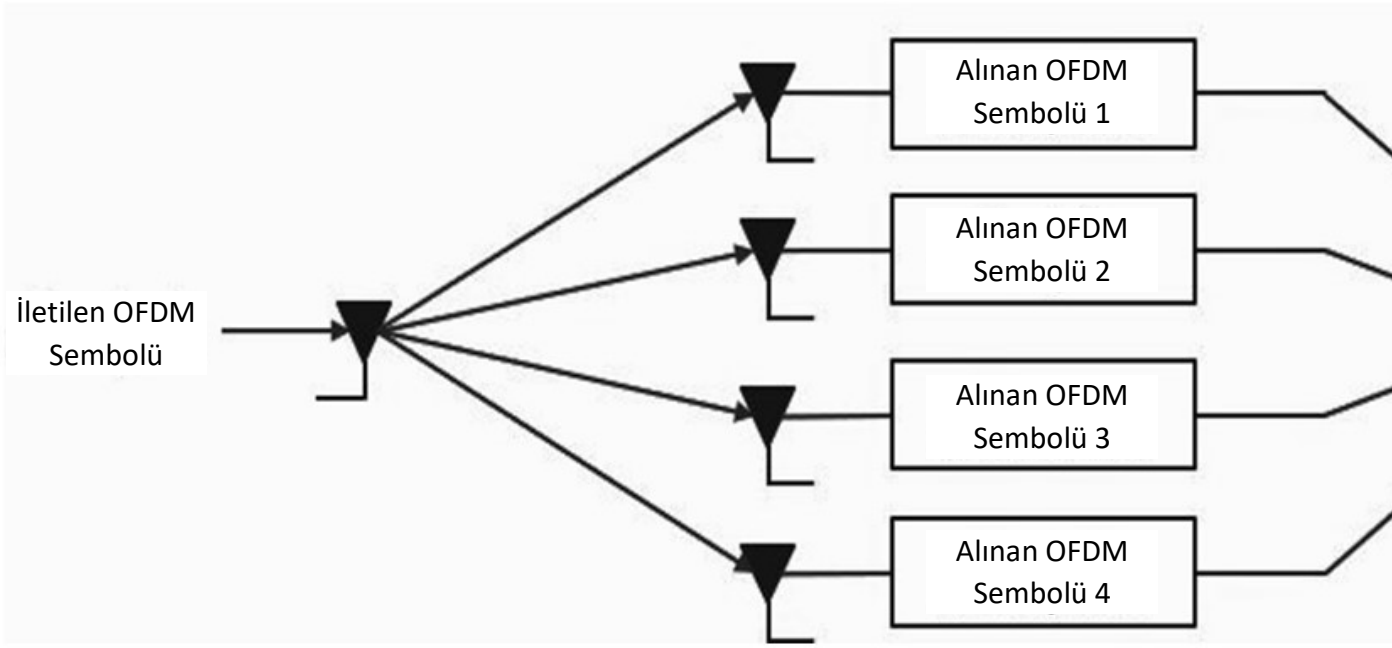
ŞEKİL 6


Pilot veriler
Yapay olarak kaydırılmış pilot veriler
Pilot sinyalin asıl konumuna daha ya
şekilde düzenlenen kanal üzerinden
Pilot sinyalin asıl konumu ve yapay
eşik mesafeler
Pilot sinyalin asıl konumu ve yapay
versiyonu arasındaki eşiğin üzerinde

ŞEKİL 7


Pilot veriler
Yapay olarak kaydırılmış pilot veriler
Pilot sinyalin asıl konumuna daha ya
düzenlenen kanaldan geçirilen pilot
Pilot sinyalin asıl konumuna daha uz
düzenlenen kanaldan geçirilen pilot
gürültüden etkilenmiş
gürültüden etkilenmiş

ŞEKİL 8


İletilen OFDM Sembolü
Alınan OFDM Sembolü 1
Alınan OFDM Sembolü 2
Alınan OFDM Sembolü 3
Alınan OFDM Sembolü 4

ŞEKİL 9